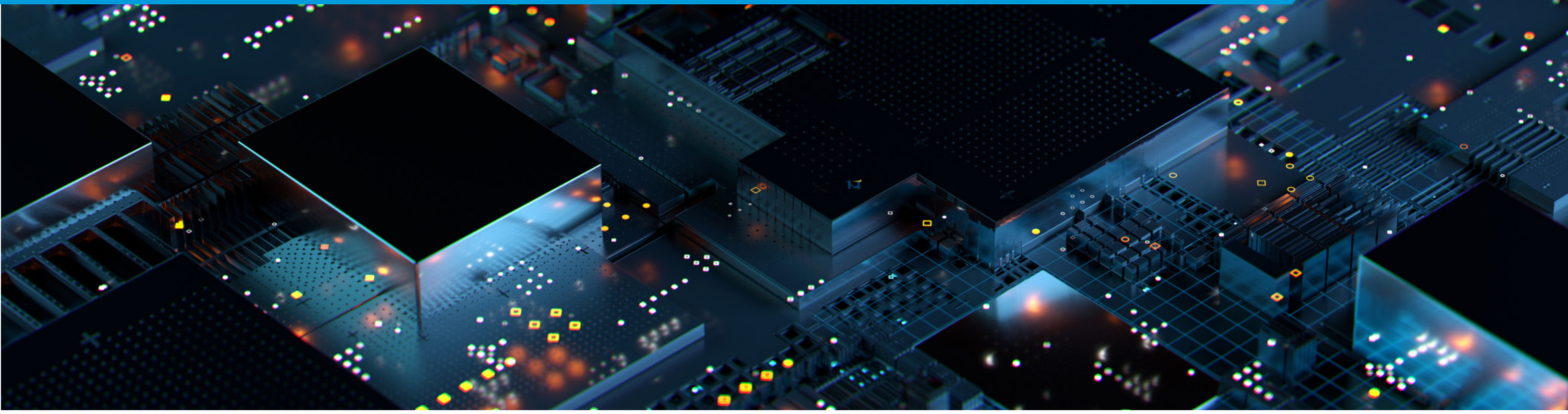
REPORT–MAY 2021

Threat Intelligence Report

2020 Threat Landscape

North-by-South-West: See What Evaded the Perimeter

VMware Threat Analysis Unit



Threat Intelligence Report

2020 Threat Landscape

Executive Summary

Today's reality is that security breaches are a given. Sophisticated attackers are too numerous and too determined to get caught by perimeter defenses. It's relatively easy to take advantage of vulnerabilities on the edge of the network or trick a user into granting access to their device. From there, attackers can lay in wait for days, weeks, or months until the time is right to spread to other more critical systems, deliver a malicious payload, and execute their objective—whatever that may be. It's not a matter of if an attack will be successful, it's a matter of when. Organizations are better served by a security team that shifts its focus from preventing all attacks to stopping the spread of attacks once they make that initial breach.

The data bears this out.

The following report from the VMware Threat Analysis Unit is a summary of key data and findings observing millions of networks/network segments from July 2020 to December 2020. It highlights threats that evaded perimeter defenses and were identified by VMware sensors placed inside the perimeter.

The findings are clear: despite a cadre of perimeter defenses being deployed, malicious actors are actively operating in the network. The research presents a clear picture of how attackers evade perimeter detection, infect systems, and then attempt to spread laterally across the network to execute their objective. Armed with this knowledge, chief information security officers (CISOs) and network security teams can gain critical insight into how to combat these threats, stop their spread, and help prevent them from doing real damage once they are inside the network.

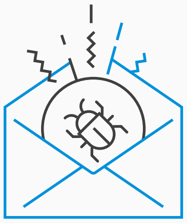
The Analysis Includes

Artifact telemetry from NSX Advanced Threat Analyzer, a network sandbox delivering a unique malware isolation and inspection environment that emulates the entire host

Network telemetry from NSX Advanced Threat Prevention, which includes network traffic analysis and intrusion detection and prevention

Additional in-depth threat analysis of real attacks launched in the second half of 2020

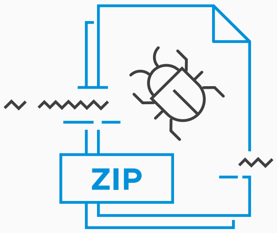
Key Insights



EMAIL CONTINUES TO BE USED AS THE MOST COMMON ATTACK VECTOR TO GAIN INITIAL ACCESS WITH MORE THAN FOUR PERCENT OF ALL BUSINESS EMAILS ANALYZED CONTAINING A MALICIOUS COMPONENT

Insight

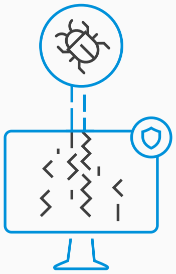
Malicious email authors are clever and relentless, and they are constantly developing new, or at least different ways to deceive and attack us. Although the malicious payloads found in email-based attacks frequently change, the vast majority of cybercriminals primarily use three basic strategies: Malicious attachments, links to malicious web pages, and enticements to perform transactions. Perimeter security solutions such as anti-virus, anti-malware, and anti-phishing tools are ineffective against advanced email-based threats, and malicious actors will continue to use email as an attack vector.



MORE THAN HALF OF ALL MALICIOUS ARTIFACTS ANALYZED WERE DELIVERED BY A ZIP ARCHIVE

Insight

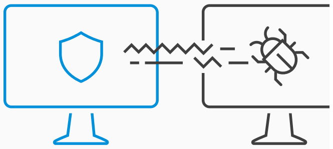
Attackers massively scaled up their operations via email campaigns weaponizing ZIP file attachments with malicious content. Attackers are well-aware of the fact that traditional sandboxing tools also lack the ability to analyze rare and esoteric files—making these tools largely ineffective for threat detection. Many security solutions treat password-protected ZIP files as encrypted files and bypass the inspection. A more modern sandboxing tool is needed to identify these threats, one that can deconstruct as many file types as possible.



DEFENSE EVASION IS THE MOST ENCOUNTERED MITRE ATT&CK® TACTIC USED BY MALWARE, FOLLOWED BY EXECUTION AND DISCOVERY

Insight

Threat actors first order of business is to evade detection. Once achieved, it's essential they become persistent within an environment by executing malicious artifacts. Once persistent, discovery of system processes and network assets commence. When attackers compromise an asset in a network, that device usually is not their ultimate destination. These tactics all occurred behind the firewall, meaning these threats have already evaded perimeter security controls.

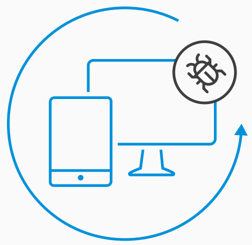


MORE THAN HALF OF THE NETWORK ANOMALIES DETECTED ARE UNUSUAL BEACONING, FOLLOWED BY CONNECTIONS ON SUSPICIOUS PORTS AND ANOMALOUS CONNECTIONS BETWEEN TWO HOSTS

Insight

Unusual beaconing is a smoking gun and constantly emits a signal to its intended target. Most communications with a beacon happen "in the clear", they aren't encrypted, and attackers are increasingly using this as a gateway within an organization's datacenter. Identifying and flagging abnormal beaconing is an effective threat detection and prevention method that can be undertaken by an enterprise security team.

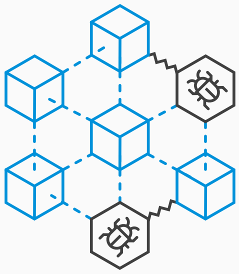
Key Insights



MORE THAN 60 PERCENT OF ALL COMMAND-AND-CONTROL SECURITY EVENTS ARE RELATED TO A COMMERCIAL REMOTE-CONTROL APPLICATION

Insight

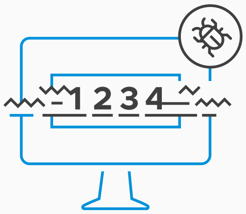
Threat actors have made an art out of hiding in plain sight. Using common management tools to communicate back to the attacker allows them to mask their transmissions alongside legitimate traffic. The problem is when you detonate a piece of malware, it does connect to bad sites but also to good sites. It does a lot of things that have nothing to do with its malicious traffic, with the command-and-control, exploit or exfiltration activity. For example, it might connect to a well-known website to check Internet connectivity. Or it might connect to legitimate mail servers to send spam. If you classify every destination of traffic as malicious, you will pollute your training sets significantly. Precisely labeling threat activity and understanding which activities are command-and-control connections, which are the lateral movement connections, which are the exploits, and what are noise requires trained machine learning (ML) algorithms.



IN THE CORPORATE NETWORK, EVENTS ASSOCIATED WITH CRYPTO MINING ACTIVITY ACCOUNT FOR A QUARTER OF ALL KNOWN THREATS

Insight

There certainly are potential risks of having the network compromised by crypto mining malware. It's not just data or intellectual property that's at stake. Many security threats exploit network resources for malicious gain. Criminals could – to borrow a phrase from enterprise sales jargon – land and expand, which means to get an initial set of malware components installed and the command-and-control channel operational, and then subsequently download more aggressive malware. Or they could sell their compromised systems to other criminals with other intents.



THE MOST COMMON BAD SECURITY PRACTICE DETECTED IS THE USE OF CLEAR-TEXT PASSWORDS

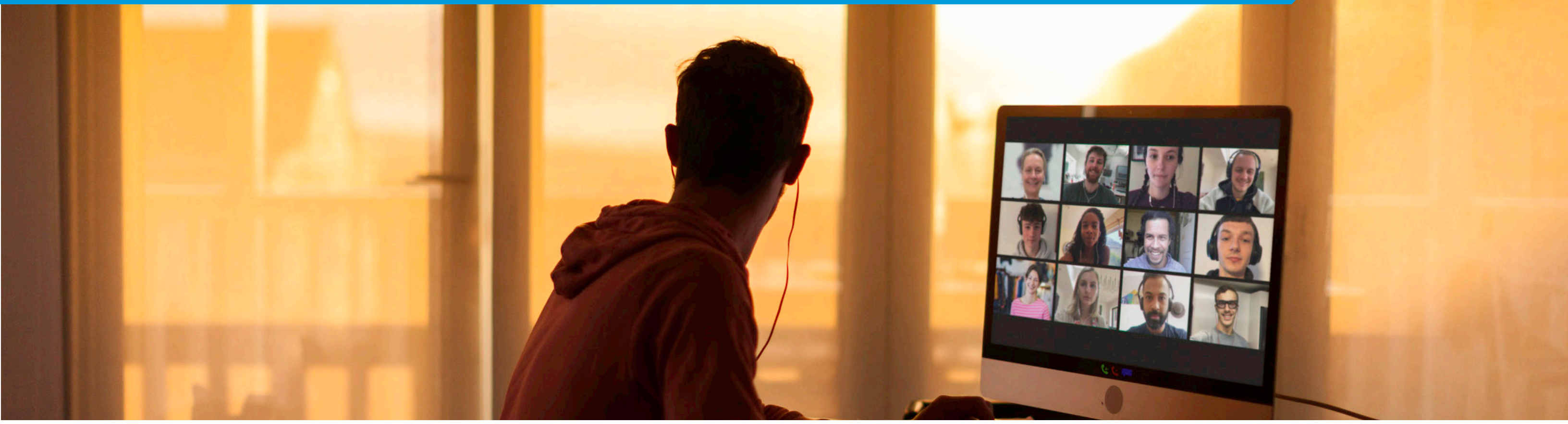
Insight

These security events are easily preventable. Transmitting clear-text passwords over the network can provide attackers the keys to the kingdom, enabling them to move laterally and exfiltrate data.

MORE THAN 75 PERCENT OF LATERAL MOVEMENT EVENTS IDENTIFIED WERE CONDUCTED USING REMOTE DESKTOP PROTOCOL (RDP)—OFTEN USING STOLEN CREDENTIALS TO LOG IN TO OTHER HOSTS ON THE NETWORK

Insight

While there are several different ways to propagate laterally, logging into hosts via Remote Desktop Protocol (RDP) using either exposed clear-text passwords via the network (see above stat), valid accounts or brute-forced credentials is still the most common technique. When attackers compromise an asset in a network, that device usually is not their ultimate destination. To accomplish their goal, bad actors are likely to break into a web server, employee endpoint device, or some other location. They'll then move laterally from this initial compromise of device through the network to reach their intended target. The initial compromise seldom causes severe damage. If security teams can detect the lateral movement before the attackers reach their intended targets, they can prevent the attacker from accessing the sensitive data. Enterprise security teams can use artificial intelligence (AI) and machine learning (ML) to determine abnormal RDP connections.



Introduction

2020 changed the way people work in unimaginable ways. The COVID-19 global pandemic and resulting economic impact pushed users away from the safety and security provided by perimeter defenses. Many people started working from home, accessing critical business systems through VPN connections or directly to Software as a Service (SaaS) platforms and other cloud apps.

Threat actors immediately took advantage of the situation, using pandemic anxiety as a trigger for social engineering attacks. These attacks increasingly focused on the delivery of ransomware, especially targeting high-profile victims. In addition, there has been a resurgence of dated exploits, likely targeting poorly maintained computers.

The main problem caused by these compromised hosts, even though they are not physically on an organization's premises, is that they may provide access to higher-privileged accounts and hosts within corporate networks, as well as enterprise data centers. In some incidents, attackers are using previously compromised user devices to gain access to Windows Domain Controllers that are then used as an incredibly effective mechanism for the distribution of ransomware components across the network. In addition, the pandemic has boosted the use of Virtual Desktop Infrastructure (VDI), Remote Desktop Protocol (RDP), and Desktop-as-a-Service (DaaS)—creating a new mix of application and user traffic within the data center.

Given these changes, it is critical for enterprise security teams to extend threat detection and prevention capabilities beyond the firewall to cover all East-West traffic.

The following insights were derived from data collected from July to December 2020 by VMware sensors deployed across a wide variety of enterprise networks. These networks are large and small and cover a wide range of industry sectors. The VMware sensors are almost always deployed behind perimeter firewalls and in the data center—providing unique insights into attacks that have already breached perimeter defenses. These highly evasive, sophisticated, and targeted attacks are actively trying to spread and deliver malicious payloads to exfiltrate data.

Artifact Telemetry

The network sandbox delivers a unique isolation and inspection environment that emulates the entire host, including CPU, system memory, and all input and output devices. This works by interacting with malware to safely analyze behaviors and provides analysis of malware artifacts evading the perimeter and traversing your data center. Over this six-month period, the Advanced Threat Prevention (ATP) offering in the NSX Service-defined Firewall (SDFW) solution gained valuable insights into how artifacts tried to infiltrate end devices.

There are three classes of artifacts: benign, suspicious, and malicious. Benign artifacts (e.g., documents, executables, libraries) do not pose an active threat. Suspicious artifacts are mostly low-risk nuisances but should not be discounted, as their nature might change with the flick of a switch (or the push of an update). Malicious artifacts are the most aggressive and destructive components, often delivered through a multi-step process whose goal is to confuse detection systems and hide malicious actions among the background noise of network events.

The percentage of occurrence of these classes of artifacts has remained relatively constant during this period. As the figure below shows, the percentage of malicious artifacts detected is around 0.1 percent.

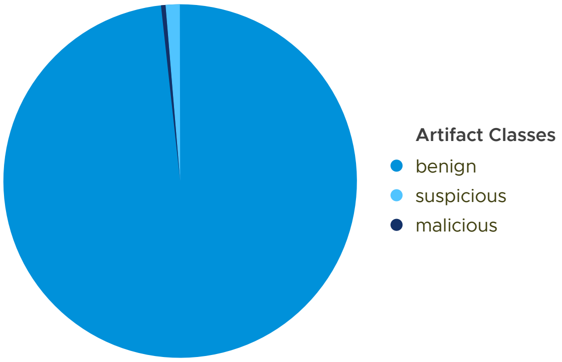


FIGURE 1: PERCENTAGES OF BENIGN, SUSPICIOUS, AND MALICIOUS FILES OVER THE ENTIRE REPORTING PERIOD.

Analyzing the most common file types observed, there's a clear difference between benign artifacts and malicious artifacts: while benign artifacts are mostly well-known and well-understood file types (such as PDF files, as shown in Figure 2), malicious artifacts rely on a number of rarer esoteric file types such as ISO9660 files and ACE archives (see Figure 3).

The use of uncommon file types to deliver malicious artifacts is in part due to the attempt to hide content in difficult-to-analyze packages and sometimes in order to exploit security flaws in unpatched, outdated software that is used to manage these types of file.

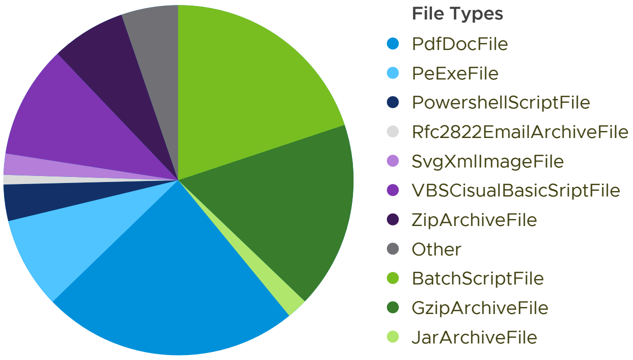


FIGURE 2: TOP FILE TYPES OBSERVED FOR BENIGN ARTIFACTS.

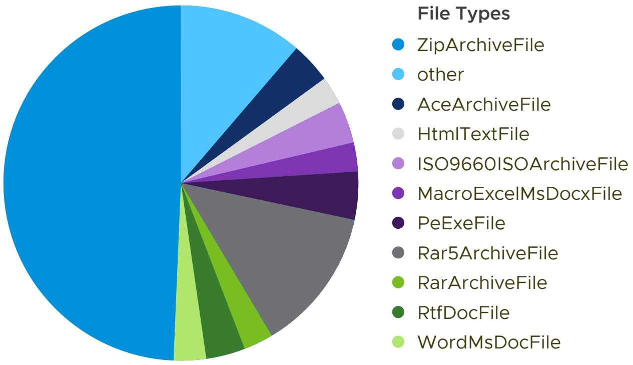


FIGURE 3: MOST COMMON FILE TYPES FOR MALICIOUS ARTIFACTS.

The chart in Figure 4, below, shows the percentage of malicious artifacts observed during the analyzed time period. Throughout the whole period, the observed percentage of malicious artifacts is less than 0.5 percent, except for two peaks that occurred during the months of June and November. The first peak (in June) represents a malicious spam campaign delivering the Avaddon ransomware. The threat actor used ZIP archives containing malicious JavaScript files. The malicious JavaScript files launch a PowerShell command that retrieves and executes the ransomware payload. The second peak (in November) was caused by a malicious spam campaign carried out by the Phorpiex botnet. The threat actor distributed ZIP archive files containing malicious executables that download and execute the BitRansomware malware [1].

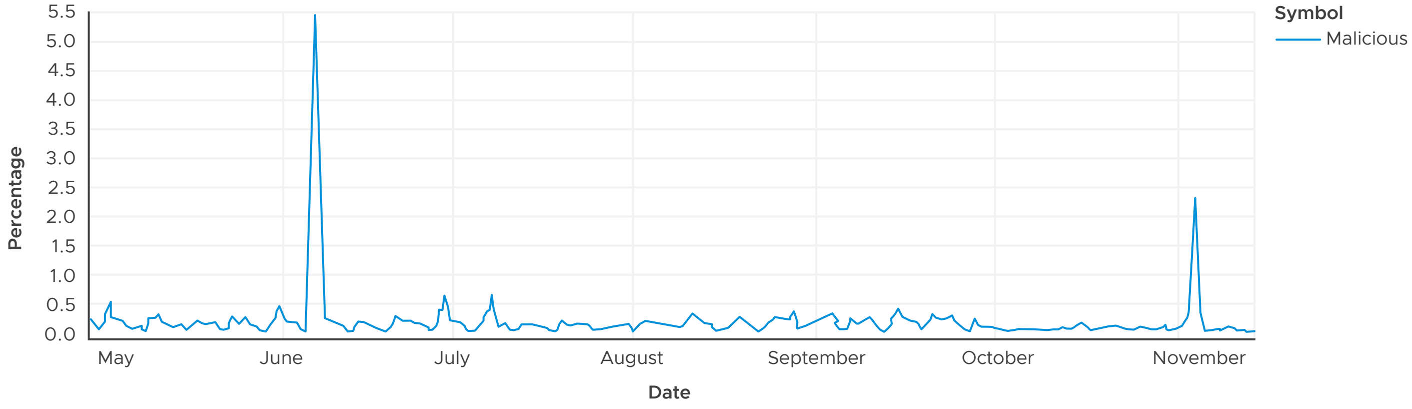


FIGURE 4: PERCENTAGE OF MALICIOUS ARTIFACTS OBSERVED DURING THE TIME PERIOD.

To better understand how attackers leverage various delivery vectors, we analyzed the malicious and suspicious file encounter rates per each delivery vector based on the telemetry data generated by organizations in the US and EMEA regions over the whole period, as shown in Figure 5. The data shows the most common vector used to deliver malware is email, which has a malicious encounter rate close to four percent. This is not surprising. Email is still the most common communication mechanism for organizations, and, as a result, can lead to better infection rates compared to other vectors. On the other hand, SMB exhibits the highest suspicious encounter rate across all vectors with over three percent of all files transferred via SMB labeled as suspicious. The investigation shows that the majority of those files are IT management tools such as batch scripts that are shared via SMB by IT for Windows updates. Threat actors have been known to leverage both file types to spread malware in the past, therefore these kinds of files are tagged as suspicious.

Keeping in mind the introduction of this report, these threats delivered via the vectors identified below were detected behind the perimeter firewall. Deploying a network sandbox to inspect artifacts in addition to perimeter controls would likely reduce infection rates.

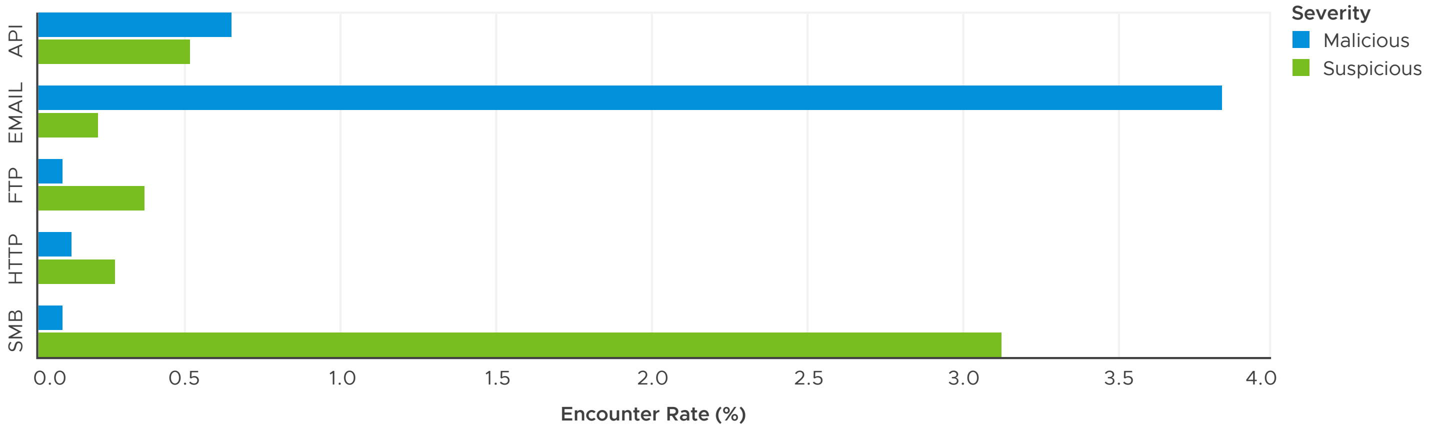
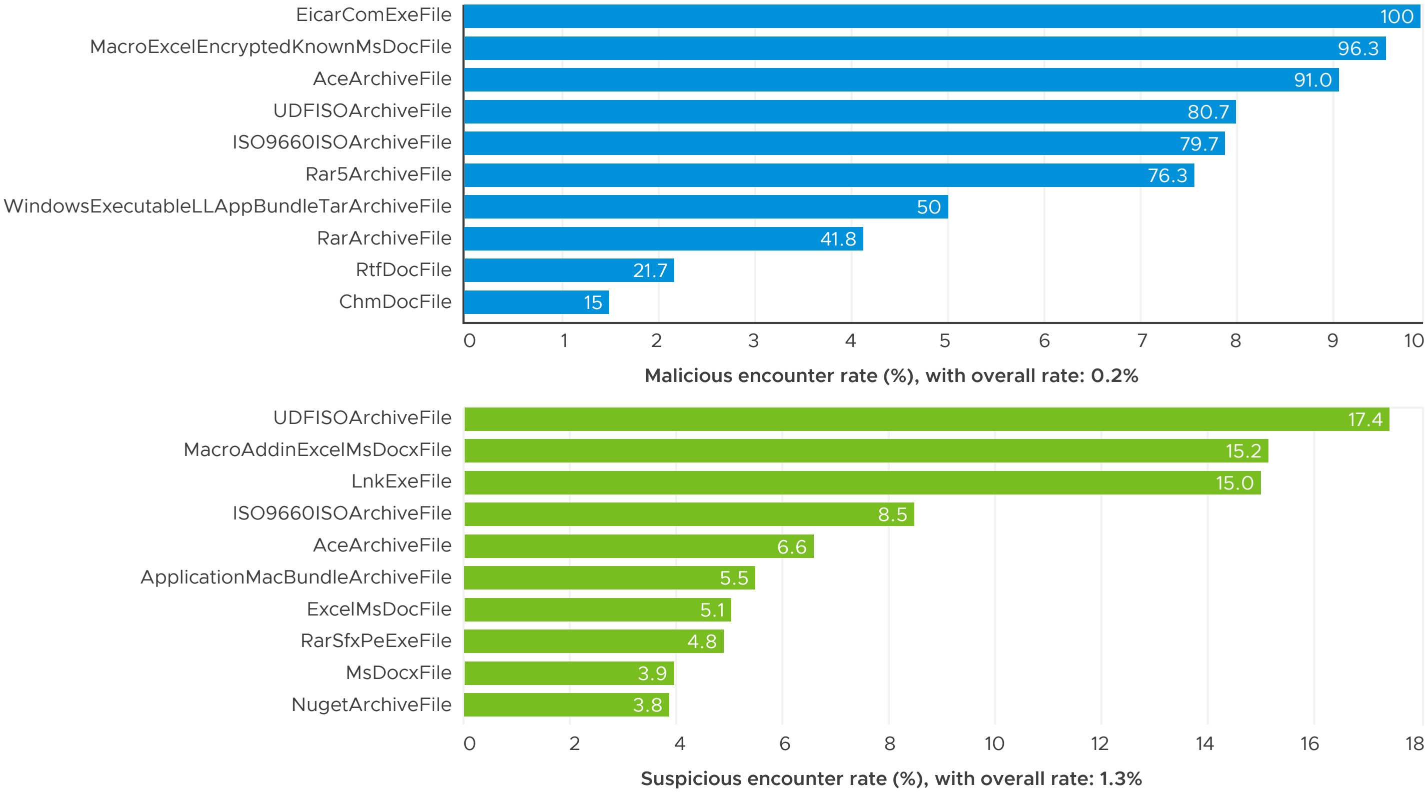


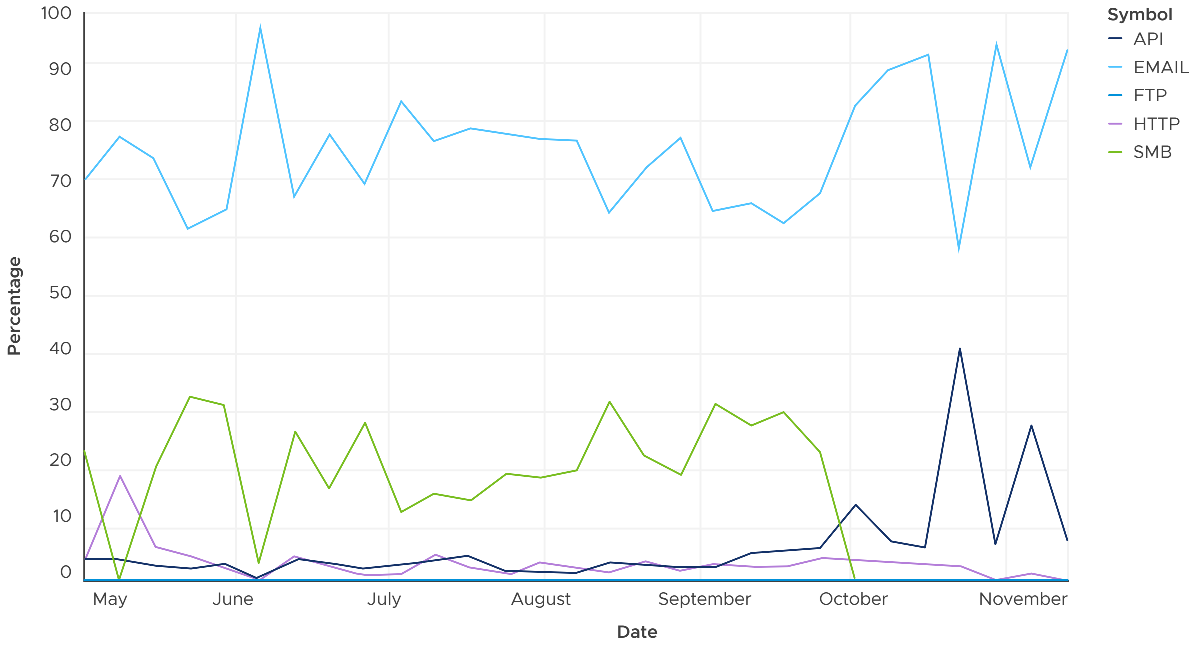
FIGURE 5: PERCENTAGES OF MALICIOUS AND SUSPICIOUS FILES PER DELIVERY VECTOR FOR THE WHOLE PERIOD.

The overall suspicious encounter rate of all file types is around 1.3 percent during this period. The lower chart in Figure 6 lists the top file types with the highest suspicious encounter rates. The top place is taken by the universal disk format (UDF) image file type (named UDFISOArchiveFile in the chart), which has a 17.4 percent suspicious encounter rate. It is worth noting that this file type has the fourth highest malicious encounter rate as shown in the upper plot. As a result, it is not surprising to see it having a high suspicious encounter rate. Similarly, other types of archives listed in the upper chart also exist in the lower plot. File type MacroAddinExcelsDocxFile comes in second on the chart with a 15.2 percent suspicious encounter rate. Attackers are known to heavily leverage malicious macros embedded in Microsoft Excel files to spread malware, such as the Emotet campaign reported at the end of 2020 [3]. On the other hand, macros are widely used for legitimate applications. Often, those macros exhibit characteristics that are similar to those of their malicious cousins, such as automatically running the macro when opening an Excel file and obfuscation to protect VBA code against copying and modification. This largely accounts for the high suspicious encounter rate.

The encounter rates and types of files for benign and malicious are vastly different. Deploying a network sandbox to inspect email attachments or setting up email rules to quarantine MacroExcelEncryptedKnownMSDocFile and AceArchiveFiles given these encounter rates is highly recommended.



The following chart, in Figure 7, shows the timeline trends of the malicious artifacts observed per delivery vector during the time period. The majority of the malicious artifacts that are observed in the telemetry are delivered through email, which indicates that spear-phishing emails are the most common method used by threat actors to deliver malicious artifacts. Sometimes the peaks observed on the delivery vector lines represent campaigns using that delivery vector. For example, the peak observed in the email delivery vector during the month of June represents the malicious spam campaign that delivered the Avaddon ransomware.



The chart in Figure 8 shows the timeline trend of the malicious artifacts encounters per filetype. The graph shows the top five file types used by the threat actors to deliver malicious artifacts during the period observed. The telemetry shows that during the analysis the bulk of the malicious artifacts were delivered in the form of ZIP archives, which were the files used in the attachments of several email campaigns.

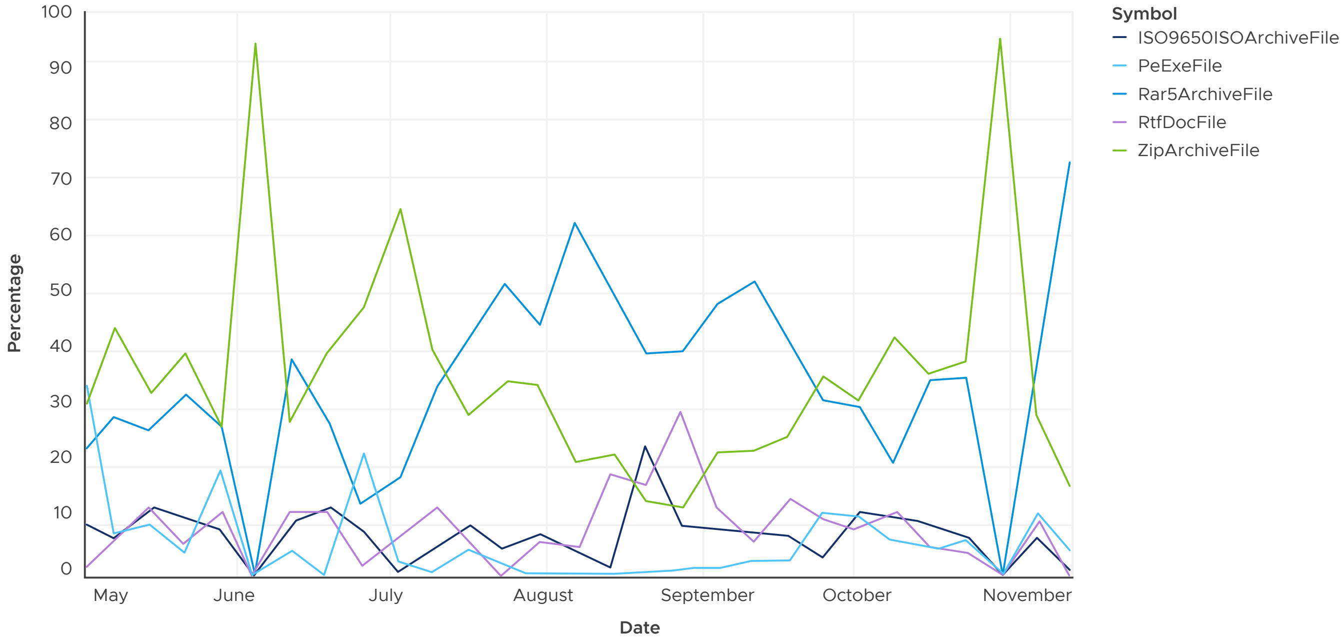


FIGURE 8: TOP FIVE MOST OBSERVED MALICIOUS FILE TYPE ENCOUNTERS DURING THE TIME PERIOD.

While delivery vectors and file types are important when evaluating the risk associated with specific artifacts, it is also interesting to look at the behavior associated with artifacts and attacks.

Figure 9 and Figure 10 show the top MITRE ATT&CK® tactics and techniques used during the period. As Figure 9 shows, TA0005: Defense Evasion is the most encountered tactics used by malware, followed by TA0002: Execution and TA0007: Discovery. In the Emotet campaign that was recently analyzed [3], the malware exhibits most of the tactics shown in the chart. The malware attempts to evade detection (TA0005: Defense Evasion) by spawning PowerShell processes and modifying executable files in the Microsoft Windows system directory on the victim's machine. The malware additionally drops an executable file (TA0002: Execution), and it enumerates running processes (TA0007: Discovery) to execute untrusted code in Microsoft Office process (again TA0002: Execution).

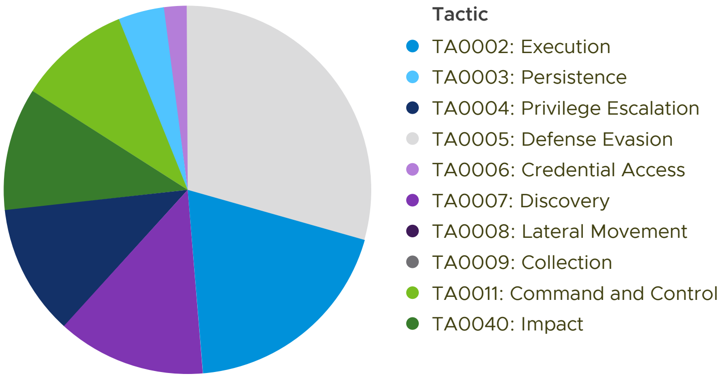


FIGURE 9: TOP MITRE ATT&CK TACTICS FOR THE WHOLE PERIOD.

Figure 10 shows the top 20 techniques over the same period. The most popular technique is T1071: Standard Application Layer Protocol. This technique is related to network activities such as downloading files from a remote location or connecting to Command-and-Control servers. This is very common in attacks that use initial payloads to carry out further malicious activities. The second most common technique is to leverage Windows Management Instrumentation (WMI, named T1047: Windows Management Instrumentation in the chart) as an attack vector. Attackers can use WMI to invoke malicious PowerShell processes (T1086: PowerShell) as observed in the Emotet attacks [3]. According to a report published in 2019 [4], nearly 50 percent of all malicious PowerShell processes were started through WMI, and another 40 percent were invoked directly by cmd.exe (T1059: Command-Line Interface).

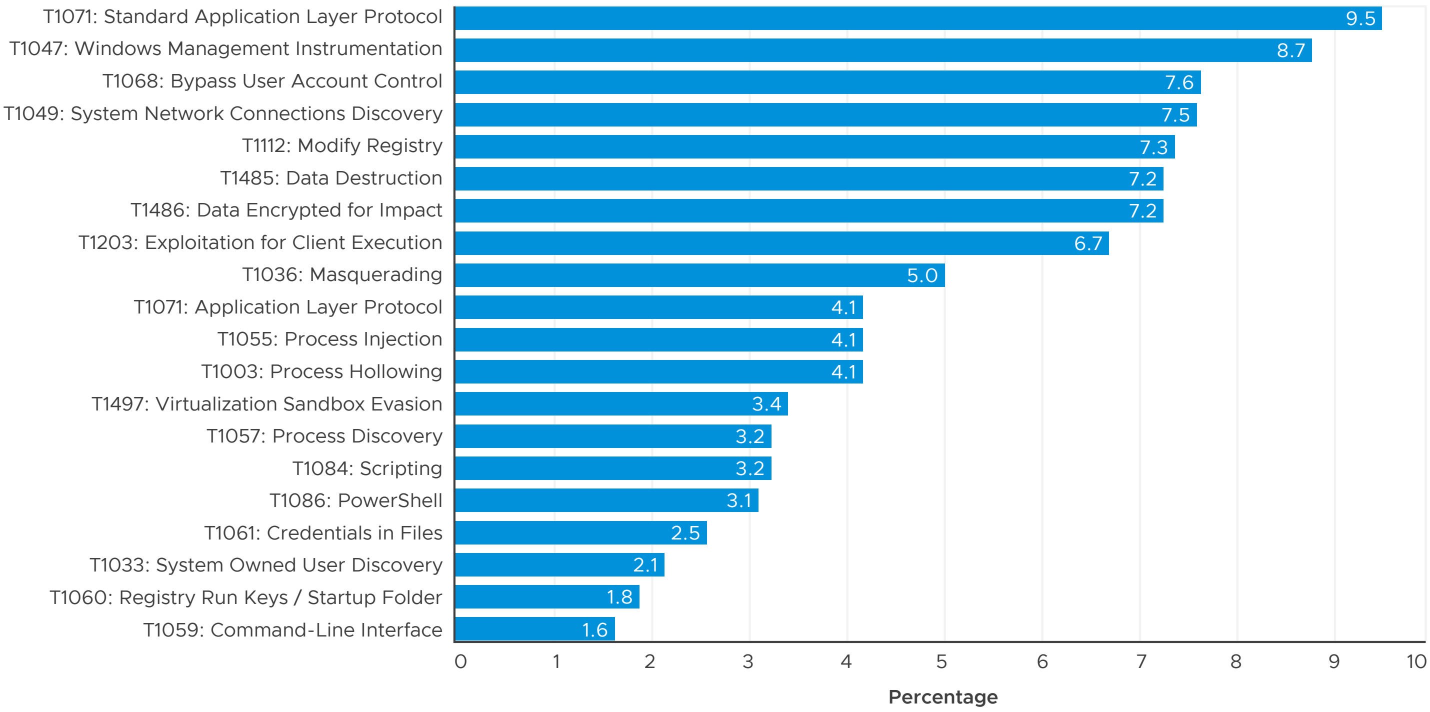


FIGURE 10: PERCENTAGE OF OCCURRENCES OF TOP MITRE ATT&CK TECHNIQUES FOR THE WHOLE PERIOD – TOTAL TECHNIQUES CONSIDERED: 68.

Network Telemetry

Analyzing network telemetry allows us to better understand the current threat landscape. The ATP offering within the NSX Service-defined Firewall (SDFW) has a broad set of detection capabilities spanning a fully distributed IDS/IPS and behavior-based network traffic analysis that helps deliver high-fidelity insights into network threats entering or moving inside the network.

Across different threat classes of events the analysis highlights the three most prevalent event types for each class. The data shows an unmitigated amount of background noise in the form of beaconing (legitimate and not) and bad security practices such as unencrypted network protocols.

Top-3 “Anomalous Network Interaction” Events

More than 50 percent of all anomalies detected by VMware sensors were unusual beaconing activities (see Table 1), meaning that the monitored corporate networks contain a number of devices contacting external endpoints or other devices on a regular basis (for both legitimate reasons and as the result of infection). Connections on suspicious ports rank second, as they are the hallmark of unauthorized attempts to access corporate resources. Ranked third, is anomalous connections between two hosts, which are events raised when, for example, a host starts accessing a service on a host that it has never accessed previously.

ANOMALY	PERCENTAGE
Unusual Beaconing Activity	58.8%
Connection on suspicious port	22.9%
Anomalous connection between two hosts	8%
Others	10.3%

TABLE 1
ALMOST 60 PERCENT OF ANOMALIES DETECTED ON CORPORATE NETWORKS ARE SOME FORMS OF BEACONING. HOWEVER, UNDERSTANDING WHICH ARE MALICIOUS AND WHICH ARE BENIGN REQUIRES SOPHISTICATED THREAT INTELLIGENCE.

Top-3 “Command and Control” Threats

This event class includes all the network detections for which the communication protocol (or the endpoints involved) can be identified with a sufficient degree of accuracy as being involved in suspicious activity. As shown in Table 2, more than 60 percent of all events are related to a commercial “Remote Control” application often used by malicious actors (as seen in the first half of 2020, including by some COVID-19 themed campaigns relying on Excel XL4 macros). The second place is held by a pen-testing/exploitation tool that is also often used by sophisticated actors (TA505). Trailing the ranking, are endpoints connecting to Command-and-Control servers to download additional payloads.

THREAT	PERCENTAGE
Commercial Remote Control Application	65.2%
Pen-Testing/Exploitation Tool	15.3%
Endpoints connecting to Command-and-Control Servers	9.1%
Others	10.4%

TABLE 2
MANY SECURITY TOOLS, SUCH AS COMMERCIAL REMOTE CONTROL APPLICATIONS AND PEN-TESTING TOOLS ARE USED BY BOTH THE BAD GUYS AND THE GOOD GUYS, AND THEREFORE UNDERSTANDING THE CONTEXT OF THESE DETECTIONS IS KEY TO EVALUATE THEIR IMPACT ON AN ORGANIZATION’S NETWORK.

Top-3 “Known Threats” Threat Classes

Table 3 lists threat classes besides “Command and Control” still detected by non-probabilistic signatures or non-ML detectors. The top three classes are all violations in some sense: bad security practices, policy violations, and crypto mining activity. Other threat classes (represented by “Others”) are all below the 10 percent threshold.

Crypto miners can devour network’s resources. From servers to desktops these threats can affect an organization’s productivity and cloud costs. In the corporate network, events associated with crypto mining activity can account for a quarter of all threats.

THREAT CLASS	PERCENTAGE
Crypto Mining	24.8%
Bad Security Practice	20.2%
Policy Violation	17.8%
Others	37.2%

TABLE 3
KNOWN THREAT CLASSES.

Top-3 “Bad Security Practices” Threats

The most common bad security practices is the lack of proper encryption (see Table 4). The most prevalent is the adoption of email servers and clients relying on clear-text password transmission, followed by the same issue with FTP. HTTP Basic Authentication (a type of HTTP authentication that relies on clear-text passwords) is the third most common bad security practice.

The simplest remedy is to remove the use of all plaintext credentials.

THREAT	PERCENTAGE
POP3/SMTP Clear-Text Password Transmission	49.3%
FTP Clear-Text Password Transmission	20.6%
HTTP Basic Authentication	15.7%
Others	14.4%

TABLE 4
ARE THE SERVICES IN YOUR NETWORK FOLLOWING BEST PRACTICES? 90 PERCENT OF EVENTS ASSOCIATED WITH BAD PRACTICES ARE LINKED TO THE USE OF PLAINTEXT CREDENTIALS.

Top-3 “Policy Violations” Threats

The most common policy violations are related to using the BitTorrent protocol (most commonly used for file sharing) in a corporate setting or loading gaming clients. The third policy violation (DNS-over-HTTPS) might be a side-effect of web browsers turning this feature on by default in corporate settings. Much of all other policy violations (in the “Others” category in Table 5) are related to VPN traffic, which is often used to evade corporate firewalls and access sensitive data.

These policy violations might lead to malicious activity, often impact productivity, and can invite copyright infringements.

THREAT	PERCENTAGE
Gaming Client	35.4%
uTorrent	26.9%
DNS-over-HTTPS	13.6%
Others	24.1%

TABLE 5
NETWORK POLICY VIOLATIONS CAN GENERATE HUNDREDS OF THOUSANDS OF EVENTS IN THE CORPORATE NETWORK. BITTORRENT AND GAMING CLIENT CAN ACCOUNT FOR MORE THAN 50 PERCENT OF ALL POLICY VIOLATIONS IN CORPORATE NETWORKS.

Top-3 “Lateral Movement” Techniques

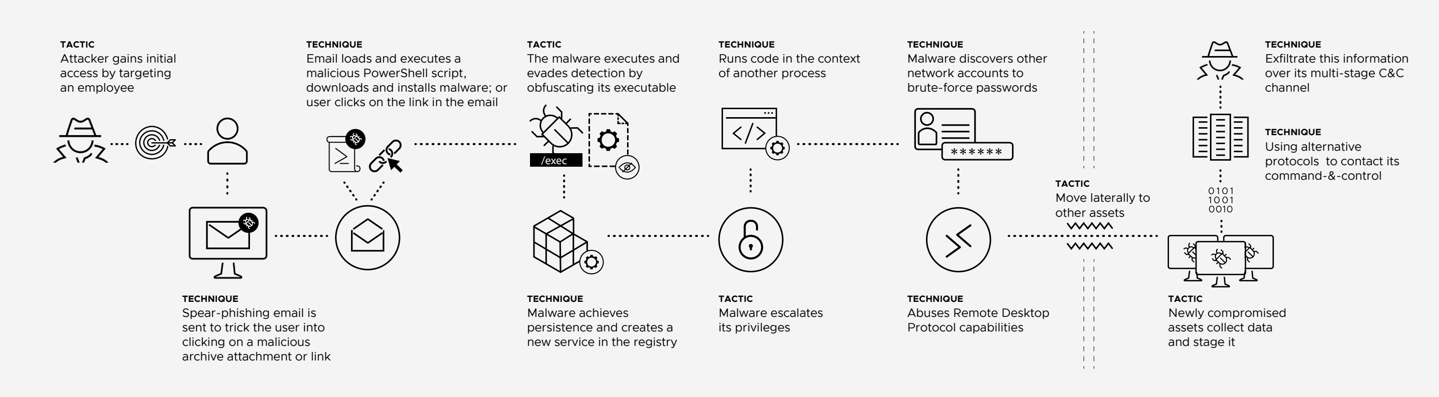
Although not related to a specific threat or threat class, below is the analysis of all network events known to exercise one of the most impactful MITRE ATT&CK® tactics in the context of network security: TA0008, Lateral Movement. As shown in Table 6, while the majority of network events were classified as employing RDP to log in into other hosts using possibly stolen credentials, more than 10 percent of detections were related to Pass the Hash, a technique used to bypass standard authentication mechanisms requiring cleartext password by relying on encrypted credentials (usually retrieved by directly accessing system memory). Interestingly, exploiting remote services via the infamous ETERNALBLUE exploit or other SMB-based exploits trails the list with a meager 2.0 percent.

THREAT	PERCENTAGE
T1076: Remote Desktop Protocol	76.5%
T1075: Pass the Hash	12.7%
T1210: Exploitation of Remote Services	2.0%
Others	8.8%

TABLE 6
WHILE THERE ARE SEVERAL DIFFERENT WAYS TO LATERALLY PROPAGATE, LOGGING INTO HOSTS VIA RDP USING EITHER VALID ACCOUNTS OR BRUTE-FORCED CREDENTIALS IS STILL THE MOST COMMON TECHNIQUE.

Counter Evasive Security Threats with VMware Solutions

These threat behaviors can be summed up thusly


TACTIC
Attacker gains initial access by targeting an employee
TECHNIQUE
Email loads and executes a malicious PowerShell script, downloads and installs malware; or user clicks on the link in the email
TACTIC
The malware executes and evades detection by obfuscating its executable
/exec
TECHNIQUE
Runs code in the context of another process
TECHNIQUE
Malware discovers other network accounts to brute-force passwords
******
TECHNIQUE
Exfiltrate this information over its multi-stage C&C channel
TECHNIQUE
Using alternative protocols to contact its command-&-control
TACTIC
Move laterally to other assets
0101
1001
0010
TECHNIQUE
Spear-phishing email is sent to trick the user into clicking on a malicious archive attachment or link
TECHNIQUE
Malware achieves persistence and creates a new service in the registry
TACTIC
Malware escalates its privileges
TECHNIQUE
Abuses Remote Desktop Protocol capabilities
TACTIC
Newly compromised assets collect data and stage it

VMWARE'S NSX SERVICE-DEFINED FIREWALL WITH ADVANCED THREAT PREVENTION (ATP) CAN PREVENT INITIAL ACCESS BY DETECTING MALICIOUS ARTIFACTS AND LINKS THAT ATTEMPT TO TRICK USERS. VMWARE'S ENTERPRISE CLASS FILE ANALYSIS CAPABILITIES USE DEEP CONTENT INSPECTION TO DETECT ADVANCED THREATS PERSISTING, ESCALATING PRIVILEGES, AND EVADING DETECTION. NETWORK TRAFFIC ANALYSIS USES DEEP UNDERSTANDING OF MALICIOUS BEHAVIORS TO DISCERN BETWEEN BENIGN ANOMALIES AND MALICIOUS LATERAL MOVEMENT, ACCOUNT DISCOVERIES, AND BRUTE-FORCE TECHNIQUES. NETWORK TRAFFIC ANALYSIS AND DISTRIBUTED IDS/IPS WORK TOGETHER TO DETECT AND RESPOND TO ALTERNATIVE PROTOCOLS USED TO COMMUNICATE AND EXFILTRATE DATA.

Instead of solely trying to stop the inevitable with physical perimeter hardware appliances, enterprise security teams should also focus their efforts on blocking lateral movement once bad actors make that initial breach. This requires a fundamental change in how security is done with an approach that requires the operationalizing of East-West security at scale.

VMware's NSX Advanced Threat Prevention (ATP) offering for the *NSX Service-defined Firewall* (SDFW) delivers the broadest set of threat detection capabilities that span network IDS/IPS and behavior-based network traffic analysis. This also includes VMware *NSX Advanced Threat Analyzer*™, a sandbox offering based on a full-system emulation technology that has visibility into every malware action. VMware NSX is purpose-built to protect data center traffic with the industry's highest fidelity insights into advanced threats.

- Network traffic analysis (NTA) applies unsupervised machine learning (ML) to your network traffic to detect protocol and traffic anomalies. NTA also uses supervised ML to automatically create classifiers that recognize malicious network behaviors and previously unknown malware.
- NSX applies AI to the malicious behaviors and malware samples collected from sensors across NSX global threat intelligence network to automatically create and push new IDS/IPS signatures to all NSX sensors at machine scale.
- The patented NSX Advanced Threat Analyzer deconstructs every behavior engineered into a file or URL to determine if it is malicious. NSX Advanced Threat Analyzer sees all instructions that a program executes as well as all memory content and all operating system activity.

Conclusion

It's clear that attackers are evading the perimeter. The analysis shows attackers are using advanced evasion techniques to get around security controls, and, once in, they are able to spread undetected and undeterred until they accomplish their objective—whether that is stealing information or causing disruption. Enterprise security teams need a new way to keep users, applications, data, and systems safe by operationalizing East-West security at scale.

VMware NSX security solutions provide the visibility necessary to detect threats inside the network, as well as the mechanisms to contain their spread and limit damage. As part of VMware's Zero Trust Architecture, *NSX SDFW* with *ATP* capabilities combined with in-host visibility and detection provided by *VMware Carbon Black EDR* offer a unique opportunity to deploy a comprehensive security solution that provides the visibility and fine-grained enforcement controls to address these threats evading the perimeter.

Additional In-Depth Threat Analyses

The VMware Threat Analysis Unit (TAU) has worked on several in-depth threat analyses.
The following analysis results were made public through blog posts and conference presentations.

Navigating supply-chain Vulnerabilities with a Zero Trust Architecture

In light of the SolarWinds breach, this analysis helps customers who may have questions on how a Zero Trust Architecture (ZTA) can act as an effective approach to limit the impact of such attacks.

Understanding the SolarWinds breach and its repercussions is a work in progress, and new details will emerge from the analysis of artifacts and telemetry.

For more information please see: Re-evaluating Your Security Posture in the Wake of the SolarWinds Breach - *https://www.vmware.com/security/solarwinds-breach.html?src=WWW_US_HPHA_SolarWindsBreach_SiteLink*

The Evolution of Microsoft Excel 4.0 (XL4) Macro Weaponization

VMware TAU observed a number of attack waves that exploited XL4 macros in order to compromise hosts. These macros are becoming increasingly popular for attackers as security vendors struggle to play catchup and detect them properly.

This technique abuses a legitimate feature of Microsoft Excel and does not rely on any vulnerability or exploit. For many organizations, blocking these files is not a viable solution and any signatures to flag these samples must be precise enough not to trigger on files that leverage this feature legitimately.

As this is a 30-year-old feature that has only been discovered and exploited en masse by attackers in the last year, many security vendors do not currently have detection mechanisms in place to trigger on these samples. Building reliable signatures for this type of attack is not a small task. Analysis shows thousands of samples leveraging this technique after monitoring and tracking their evolution for six months. Intercepting these samples has provided valuable data to build statistics, identify trends, find outliers, and track campaigns. This enables the clustering of samples into distinct waves, which clearly show how this technique has evolved over time to become more sophisticated and more evasive.

As XL4 macros represent somewhat ‘uncharted territory’, malware authors are introducing new tricks on a regular basis, pushing the boundaries of this technique, and identifying ways to evade detection and obfuscate their code. The techniques employed by these attackers include ways to evade automated sandbox analysis and signature-based detection as well as hands-on analysis performed by malware analysts and reverse engineers. As previously mentioned, these techniques appear to surface in waves, with each new wave introducing new tricks that build on the previous wave or cluster. A series of blog posts describe each wave and cluster in detail, breaking down every new technique discovered and explaining why each is significant.

The results of this research were presented at the Virus Bulletin Conference (VB2020) in October 2020.

The original blog post can be found here: *https://www.lastline.com/labsblog/evolution-of-excel-4-0-macro-weaponization/*

A follow-up blog post can be found here: *https://blogs.vmware.com/networkvirtualization/2020/10/evolution-of-excel-4-0-macro-weaponization-continued.html/*

Trick of Threat: Ryuk Ransomware Targets Healthcare Industry

In October 2020, the Cybersecurity & Infrastructure Security Agency (CISA) posted a warning about possible forthcoming ransomware attacks targeting the healthcare industry. This report raised concerns related to strained hospital and care center resources due to the pandemic. As a consequence, a ransomware attack, in addition to crippling a healthcare provider's infrastructure, might actually put the lives of patients at risk.

The advisory describes in detail the tactics, techniques, and procedures (TTPs) followed by the malicious actors. The attack uses a number of malware components, such as TrickBot, BazarLoader, Ryuk, and Cobalt Strike to compromise networks, create bridgeheads, and then move laterally so that, eventually, a ransomware attack can be successfully carried out.

The Ryuk ransomware takes a targeted approach and selects victims from businesses, hospitals, and government institutions and demands an extremely high ransom for data recovery. Ryuk uses AES-256 as the symmetric encryption algorithm and RSA 4096 as the asymmetric algorithm. In most cases, the initial steps of the attack are social engineering attacks that trick users into downloading and executing downloaders (TrickBot and BazarLoader), which, in turn, download the ransomware (Ryuk).

An in-depth analysis of the various malware components involved was performed, as well as the network evidence associated with their actions. The results show a kill-chain involving downloaders who use a long chain of execution involving diverse elements, such as DLLs and PowerShell scripts to deliver the ransomware payload.

More details about this threat can be found in this blog post: *https://blogs.vmware.com/networkvirtualization/2020/11/ryuk-ransomware-targets-health-care-industry.html/*

COVID-19 Cyberthreats and Malware Updates

VMware TAU covered COVID-19-themed attacks in two different analyses. In both cases, the analysis shows social engineering attacks that leveraged the anxiety around the pandemic.

Threat actors have indeed been very active during the current global pandemic. However, in the initial investigation carried out in May [5], it showed that their M.O. is hardly novel: they use email attachments as the initial infection method to eventually deliver information stealers or spyware. The malicious actors heavily rely on archive files since they provide a thin layer of protection against legacy or neutered security solutions that are unable to extract lesser-used archive formats and correctly process their contents.

The majority of the info stealers follows a "Malware-as-a-Service" model, and they are sold for very affordable prices in underground marketplaces. Because of this, the main differentiator between different campaigns ends up being the malware configuration rather than the code itself. Instead, what keeps changing over time is the packer entrusted to keep the malware undetected for as long as possible. The latest iterations have been delivering payloads downloaded from publicly hosted platforms (like Google Drive™ online storage service or Microsoft OneDrive) making the resulting network traffic difficult to identify and block.

As compared to the infostealer-centric attacks reported in May [5], there has been a shift to more sophisticated threats in the following months such as the modular NanoCore RAT and the infamous Emotet [6]. In the COVID-19-themed Emotet campaign, the Emotet gang abused the caption metadata within a form object to hide a malicious PowerShell script string. The general infection chain is similar to the other Emotet campaigns reported [3], but analysis also shows some different tricks in this variant such as abusing a frame control instead of a multipage object to store the PowerShell script string and using Invoke-Item cmdlet to execute the Emotet payload instead of calling the create method from win32_process class.

As the pandemic continues, expect threat actors, including the Emotet gang to keep leveraging the COVID-19 theme and evolving their TTPs to launch fresh attacks.

More details can be found in this blog post: *https://blogs.vmware.com/networkvirtualization/2020/11/covid-19-cyberthreat-and-malware-updates.html/*

Note that this blog post is the continuation of a previous analysis effort, described here: *https://www.lastline.com/labsblog/infostealers-weaponizing-covid-19/*

Defeat Emotet Attacks with Behavior-Based Malware Protection

The security community had enjoyed a few months of silence from Emotet, an advanced and evasive threat that started in February of 2020. But this silence was broken last July as VMware TAU observed a new major Emotet campaign. What caught the attention of VMware TAU was that, as a whole, the security community still lacks the capacity to effectively detect and prevent Emotet - even though it first appeared in 2014.

In the Emotet attacks discussed herein, Emotet successfully leveraged various techniques to maximize its infection rate. As seen in typical Emotet attacks, the infection process starts with a SPAM campaign using phishing emails with attached weaponized Word documents. The findings show that evasion techniques used in the attacks such as heavily obfuscated VBA macros and leveraging form controls like multipage caption to hide a malicious PowerShell script have proven to be very effective in defeating signature-based detection. This imposes great challenges to traditional security controls that depend heavily on signatures to detect threats. Instead, behavior-based approaches such as VMware's AI-driven next-gen sandboxing solution show great effectiveness in stopping attacks such as the ones that leverage the techniques discussed above.

The details of this research can be found here: *https://blogs.vmware.com/networkvirtualization/2020/11/defeat-emotet-attacks-with-behavior-based-malware-protection.html/*

VelvetSweatshop: Default Passwords Can Still Make a Difference

During the month of October and November 2020 VMware TAU observed a spike in detection of encrypted Excel files. In general, Office documents can be password-protected using a symmetric key encryption mechanism involving one password that is the key to both encrypt and decrypt the file.

Malware writers use this key as an additional evasion technique to hide malicious code from anti-virus scanning engines. The problem is that encrypting a file introduces the disadvantage of requiring a potential victim to enter a password (which is normally included in the phishing or spam email containing the encrypted attachment). This makes the email and the attachment very suspicious, thus greatly reducing the chance that the intended victim will open the encrypted malicious attachment.

However, the attackers are using an obscure feature of Excel that automatically decrypts an encrypted spreadsheet without asking for a password if the password for encryption happens to be VelvetSweatshop. This is a default key stored in Excel's program code for decryption. It is a neat trick that attackers can leverage to encrypt malicious Excel files in order to evade static analysis-based detection systems while eliminating the need for a potential victim to enter a password.

The embedded decryption key in Excel is not a secret. It has been widely reported for many years. However, seeing it still actively and extensively used made us wonder how effective modern AV scanning engines are at dealing with encrypted malicious Excel files.

Several tests were performed to see how the detection effectiveness of existing AV engines change when Excel files are encrypted, when the encryption is removed, and when a different level of encryption is used. The results were somewhat surprising. Even though the use of the default key is a known evasion technique, it is still very effective especially when using AES-256 encryption.

The details of the analysis can be found in this blog post: *https://blogs.vmware.com/networkvirtualization/2020/11/velvetsweatshop-when-default-passwords-can-still-make-a-difference.html/*

The Snake Ransomware

During the month of June 2020, VMware TAU discovered a sophisticated and targeted malware belonging to the Snake ransomware family. The malware is written in the Go language and it is heavily obfuscated. The hard-coded strings are encrypted, source code is obfuscated, and the ransomware attempts to stop anti-virus, endpoint security tools, and monitoring and correlation components.

The Snake ransomware is distributed via a focused and targeted campaign that concentrates exclusively on targeting enterprise networks. The ransomware family has ties to Iran and has historically been observed targeting critical infrastructures such as SCADA and ICS systems. More recently, the malware has been observed targeting healthcare organizations.

The ransomware in this analysis specifically targeted the corporate network of a Japanese automobile manufacturer. The ransomware appears primarily to be targeting servers as it has logic to check for the type of host it is infecting, and it attempts to stop many server-specific services and processes.

The details of the analysis can be found in this report: *https://blogs.vmware.com/networkvirtualization/files/2020/11/Targeted-Snake-Ransomware.pdf*

Phorpiex-Powered BitRansomware Targets APAC Universities

BitRansomware (also known as DCryptSoft or Readme) is, as the name implies, a ransomware program that first surfaced in July 2020. Initially targeting English-speaking users, this threat actor recently expanded its attack to the APAC region, focusing on universities in Japan and Hong Kong in particular.

Like the Nemty ransomware attack reported last year [7], the BitRansomware attack was delivered via a massive email campaign carried out by the Phorpiex botnet. The malspam campaign distributed a swarm of ZIP archive files containing ransomware downloaders in malicious executables.

As the analysis shows, the threat actor leveraged various techniques to maximize the infection rate of the attack. The attack started with a SPAM campaign, and, if the attachment was activated, it downloaded and displayed an image on the victim's screen while also downloading the actual Phorpiex variant from one of its Command-and-Control hosts. Upon execution, the Phorpiex payload dropped the final BitRansomware copy that it grabbed from a C2 server.

The details of the analysis can be found in this report: *https://blogs.vmware.com/networkvirtualization/threat-intelligence/*

Bibliography

1. J. Zhang and S. Ortolani, "Phorpiex-Powered BitRansomware Targets APAC Universities," VMware, 10 12 2020. [Online]. Available: https://blogs.vmware.com/ networkvirtualization/threat-intelligence/.
2. J. Zhang and S. Ortolani , "VelvetSweatshop: Default Passwords Can Still Make a Difference," VMware, 19 11 2020. [Online]. Available: https://blogs.vmware.com/ networkvirtualization/2020/11/velvetsweatshop-when-default-passwords-can-still- make-a-difference.html/.
3. J. Zhang, "Defeat Emotet Attacks with Behavior-Based Malware Protection," VMware, 5 11 2020. [Online]. Available: https://blogs.vmware.com/ networkvirtualization/2020/11/defeat-emotet-attacks-with-behavior-based-malware- protection.html/.
4. Symantec Security Response, "Living off the Land: Attackers Leverage Legitimate Tools for Malicious Ends," Broadcom, 24 12 2019. [Online]. Available: https:// symantec-enterprise-blogs.security.com/blogs/threat-intelligence/living-land- legitimate-tools-malicious.
5. S. Sarkar, J. Zhang and S. Ortolani, "InfoStealers Weaponizing COVID-19," Lastline (now part of VMware), 11 5 2020. [Online]. Available: https://www.lastline.com/ labsblog/infostealers-weaponizing-covid-19/.
6. J. Zhang, S. Sarkar and S. Ortolani, "COVID-19 Cyberthreats and Malware Updates," VMware, 9 11 2020. [Online]. Available: https:// blogs.vmware.com/ networkvirtualization/2020/11/covid-19-cyberthreat-and-malware-updates.html/.
7. J. Zhang and S. Ortolani, "Nemty Ransomware Scaling UP: APAC Mailboxes Swarmed by Dual Downloaders," Lastline (now part of VMware), 18 2 2020. [Online]. Available: https://www.lastline.com/labsblog/nemty-ransomware-scaling-up-apac-mailboxes-swarmed-dual-downloaders/.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 **vmware.com**