

MORPHISEC LABS THREAT REPORT | **DECEMBER 2018**

FOREWORD

Keyur Desai, CIO – Essar Ports & Shipping
Head Info-Security, Network & Communications, Essar



Threats come in different forms, and in different cycles in terms of frequency and severity. It's clear that cybersecurity is shifting to a more customized model because of this. For teams who know what their challenges are, and for teams who need to defend against the different types of threats, they know it takes a fine-grained approach to do the following:

1. Apply a process that helps filter out the threats that aren't an immediate, imminent threat to the organization.
2. Architect a highly specific approach that maps to how your organization is specifically targeted by attackers, whether by vertical industry or location that includes prevention, intelligence and remediation.

The landscape of threats continues to iterate based on IT modernization trends, access to systems and, for attackers, how quickly and efficiently they can deconstruct traditional defense techniques and technology.

Oftentimes, determining root cause is one of the more challenging and time-consuming initiatives when companies are breached, or just investigating threats. This can range from partial execution of malware, to exploited vulnerabilities that may have gone unpatched. Or in the case of a breach, data exfiltration, and exactly how that backdoor was established, set up and leveraged.

However, today, proactive security teams are looking at geopolitical events, and are able to prepare and anticipate at certain times, where attackers might strike. In addition, almost 20% of people are concerned about the possibility of a cyberattack crippling the critical infrastructure of their country.

Moreover, intelligence is critical in consistently getting better at cybersecurity. But the ability to prevent a higher volume of threats more efficiently, and with a much higher level of efficacy, is something every security practitioner strives for.

This is where innovative approaches like Moving Target Defense are changing the dynamic against attackers, and they are changing how many of us are thinking about protecting the organization we work for, as well as our own individual environments and finances.

The research out of Morphisec Labs is essential to understanding exactly what some of the key threat trends really are, and it's important for every security practitioner to explore how dedicated researchers are analyzing threats for the betterment of the market.

CONTENTS

Foreword	2
by Keyur Desai, CIO – Essar Ports & Shipping, Head Info-Security, Network & Communications, Essar	
Key Threat Findings	4
Overview	6
Focus on Finance	7
Select Attack Profiles	9
Adobe Acrobat Double-Free Vulnerability CVE-2018-4990	10
VBScript CVE-2018-8174 aka “Double Kill”	12
Mylobot	14
SharpShooter Attack	16
Cobalt Group 2.0	17
In Conclusion	19
by Michael Gorelik, Chief Technology Officer and Head of Threat Research, Morphisec	

Key Threat Findings

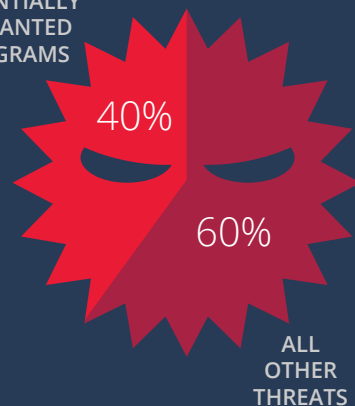
Note that Morphisec's unique focus as an advanced threat prevention solution, which is used in conjunction with antivirus, means that Morphisec threat intelligence is skewed toward threats that are able to evade antivirus:



Banking Trojans represented 25% of all attacks in Q2/Q3, up from 16.7% in Q1. Emotet held its place as the top banking malware in Q2 but disappeared from the scene in Q3, giving the lead to Trickbot. As has been true for at least the last year and a half, fileless Kovter variants account for a steady 10–15% of attacks.

Adware and potentially unwanted programs (PUPs) continue to be the largest group of threats prevented by Morphisec, representing 40% of all attacks. Much of today's adware borders on spyware and, as a threat, has potentially damaging impact and should not be dismissed. Many strains of adware are being incorporated as part of broader attacks with sophisticated, evasive techniques that can penetrate operating systems and bypass static defenses.

ADWARE &
POTENTIALLY
UNWANTED
PROGRAMS



ALL
OTHER
THREATS

Exploit kits, some which hadn't seen updating in years, are back in play, incorporating new Flash, VBScript and Acrobat vulnerabilities.

Key Threat Findings (continued)

The top ransomware threat prevented was GandCrab, with Sigma a distant second. With each new release of updated GandCrab ransomware, Morphisec sees a spike in threats prevented, which then levels out as AV and NGAV systems catch up.



Coin mining malware remained popular, accounting for 30% of attacks, with RIG-delivered miners the most prevalent type seen by the Morphisec system.

As previously stated, all attacks prevented by Morphisec in the second half of the year involved at least one fileless technique, with approximately 15% of attacks never dropping a malicious executable on disk.

Overview

The second half of 2018 continued many of the trends we observed in the first half of the year along with several new ones. Cryptominers held their position of prominence, although by the third quarter we saw the beginnings of a slowdown. Ransomware continued to decline in numbers but evolve in sophistication and impact, especially with the evolution toward ransomware-as-a-service model.

Take GandCrab ransomware, which first emerged in January 2018 as profiled in our previous Threat Report and, at the publication date of this report, was on its sixth iteration. Its developers take a 60/40 split with anyone utilizing the service, and are constantly modifying the malware and updating its techniques. In the past months GandCrab has incorporated various methods of distribution including via a rare .egg compression tactic, exploit kits, a fake Adobe Flash update site and various social engineering techniques such as fake font updates.

Banking Trojans also continued to increase. New variants of Trickbot, Emotet, Corebot, Qakbot and Kovter plagued organizations in Q2 and Q3, with updated techniques that allow them to identify and evade security tools and sandboxing environments. The most utilized techniques seen were Process Hollowing, Reflective Loading and Injection and whitelisting bypass using Rundll32, Regsvr and, recently, the RegAsm command line utility.

As predicted, the threat of vulnerabilities created by the Meltdown and Spectre CPU flaws has not faded. Side channel attack research has rushed full steam ahead and we saw the announcement of several new Spectre-class attacks. To date, all are theoretical and no Spectre-type exploits have been discovered in attacks in the wild.

The middle part of the year did bring one surprise — exploit kits are making a comeback, mainly thanks to their adoption of new Flash and Internet Explorer zero-day vulnerabilities. Many of the new zero-days are Use-After-Free vulnerabilities such as the VBScript vulnerability (CVE-2018-8174) and Acrobat Reader Double-Free Vulnerability (CVE-2018-4990) analyzed in this report. While exploit kit attacks are nowhere near their 2016 peaks, they pose a disproportionate threat as most organizations cannot patch fast enough to keep up with the quantities of vulnerabilities identified on a weekly basis, both because of operational reasons and the risk of introducing conflicts if patching is not tightly regimented.

In this expanded edition of our threat report, we also take an in-depth look at challenges facing the finance services industry. As our findings show, the finance industry is the number one target of advanced threats. And, according to a new survey, consumers indicate a fear of the consequences of such attacks.

Sophisticated Targeted Threats Originate with Nation-State Actors

The recent Flash and IE zero-day exploits are tied to the Lazarus group, the alleged North Korean group behind the infamous Sony hack and SWIFT bank heists. The allegedly Russian APT28 group has also been highly active, with an attack on the Italian Navy in July, thwarted attempts to spoof think-tank and Senate sites ahead of the election, and attacks on network infrastructure devices and home routers.

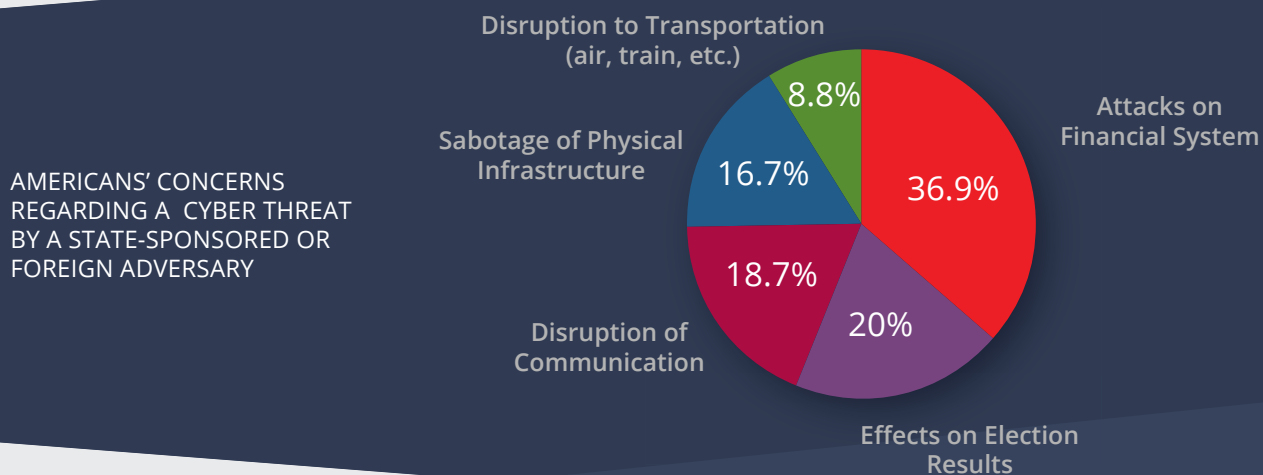
This Morphisec Labs Threat Report is based on anonymized threat data collected from approximately 2,000,000 installed Morphisec endpoint agents as well as in-depth investigations conducted by Morphisec researchers. It includes observations about trends in the wider security landscape together with analyses of the tactics and techniques used by malicious actors.

Focus on Finance

Attacks targeting the banking industry and payment records and credentials consistently topped Morphisec's threat list. This makes sense when you consider the types of attacks Morphisec catches. Sophisticated, advanced threats take time and resources to develop and to keep updated so that they remain effective at evading security solutions. Their targets are going to be those that yield big payoffs.

Take for example one of the threats profiled in the next section, a new attack by the Cobalt Group. Cobalt has been connected to the theft of millions of dollars from financial institutions worldwide. But these threats are not just a matter for banks and cybersecurity experts. The United States Department of Homeland security names financial services as one of 16 critical infrastructure sectors as attack that disrupts the delivery of financial services could have national and global economic impact.

For better or worse, the magnitude of this threat has seeped into public awareness. Recent surveys sponsored by Morphisec and conducted by independent researchers found that across all demographics, finance is number one on American citizens' minds when it comes to cybersecurity. That's ahead of attacks that bring down communications; ahead even of election security — despite the fact that the survey was conducted in the midst of the election news cycle. And while near-daily articles appeared on threats to election security, 80% of the public was still more concerned about the security of their personal financial information than their voter data.



However, this increased concern hasn't necessarily transferred to their own cyber behavior as it relates to the organizations they work for. A large segment (39.7%) never or only sometimes take cybersecurity precautions when using a work-related computer or device.

The good news (or bad depending on your perspective) — customers have not yet transferred their finance security fears into wholesale distrust of the industry. The vast majority (63.6%) believe that the financial institutions they do business with have cybersecurity measures in place to keep their money and personal information out of the hands of gangs like Cobalt.

Focus on Finance (continued)

Morphisec Threat Index Series of Enterprise and Consumer Perspectives



ABOUT 36% OF AMERICANS ARE MOST FEARFUL OF A STATE-SPONSORED CYBERATTACK ON OUR FINANCIAL SYSTEMS.

4 OUT OF 5 AMERICANS ARE MORE CONCERNED ABOUT A BREACH OF THEIR PERSONAL FINANCIAL DATA THAN THEIR VOTER DATA.



40% OF WORKERS GENERALLY DO NOT TAKE CYBERSECURITY PRECAUTIONS WHEN USING A WORK-RELATED COMPUTER OR DEVICE.

DESPITE THEIR FEARS, THE MAJORITY ARE CONFIDENT IN THE CYBERSECURITY OF THEIR FINANCIAL INSTITUTIONS.



Select Attack Profiles

Following are brief profiles of select threats that were analyzed by Morphisec Labs during the second part of 2018. It should be emphasized that Morphisec's unique moving target defense technology prevented all of the following attacks immediately upon encounter. When the Morphisec system stops an attack, it captures unique, technical data about the attack's full execution stack and memory access, which our researchers use in their investigations. In choosing which threats to profile, we generally selected threats that initially could bypass many security defenses other than Morphisec. The evasive techniques are part of what makes these threats interesting.


Two of the threats profiled in this report fall in the Use-After-Free (UAF) memory vulnerability category and additional can be found on the Morphisec blog. In general, there has been a noticeable increase in this class of vulnerabilities since the beginning of 2018. UAF vulnerabilities are particularly dangerous as they can enable full remote code execution due to easier access to read and write primitives (read and write to the full process virtual memory).

Adobe Acrobat Double-Free Vulnerability CVE-2018-4990

After a lull of four years with no exploits for Adobe Acrobat Reader, Q2 2018 saw the emergence of a new weaponized PDF. The PDF exploits two previously unknown vulnerabilities, Acrobat Reader vulnerability CVE-2018-4990 and a privilege escalation vulnerability in Microsoft Windows, CVE-2018-8120. Adobe Reader has a built-in sandbox feature that usually makes exploitation difficult. By combining vulnerabilities, this attack achieves code execution and then bypasses the sandbox protection to fully compromise the targeted system.

Potential Impact

As PDF is perhaps the most popular file format to share documents, and Acrobat Reader the most common PDF viewer, any older unpatched Windows system is vulnerable (the Windows exploit does not succeed against Windows 10 and newer). A successful compromise allows attackers to execute arbitrary code on the targeted machine and eventually assume full system control.



2018 has seen a marked rise in use-after-free exploits (double-free vulnerabilities fall within the UAF category). These types of vulnerabilities can be devastating as they result in easily achievable read and write primitives.

Adobe Acrobat Double-Free Vulnerability CVE-2018-4990 (continued)

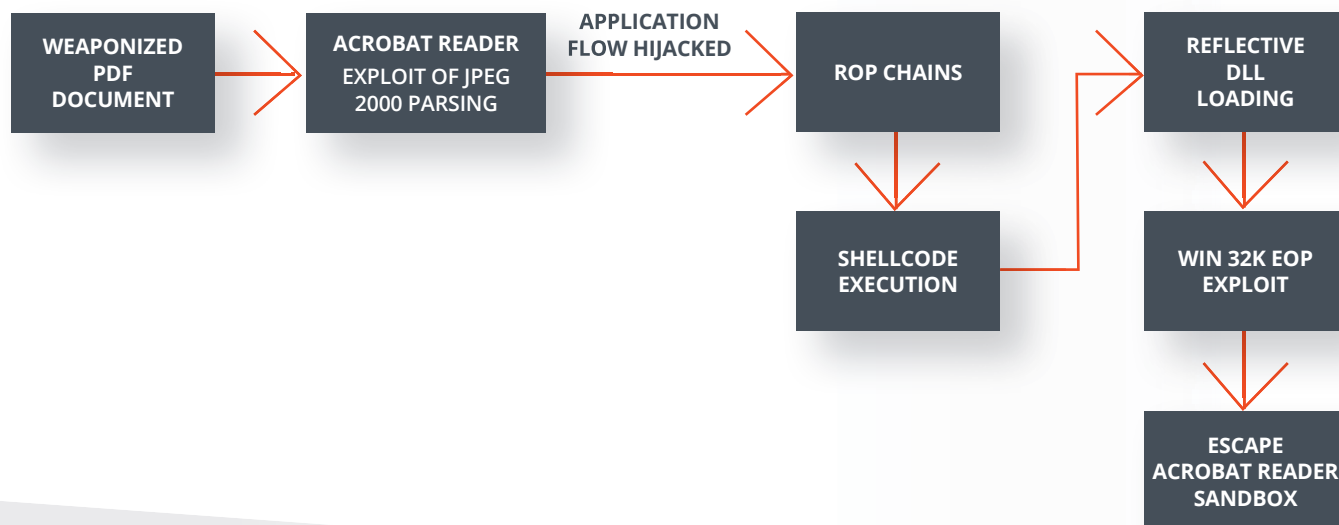
TECHNICAL DETAILS

The weaponized PDF contains two exploits: The first attacks the Adobe JavaScript engine to run shellcode in the context of that module while the second allows the shellcode to escape Adobe Reader sandbox and run with elevated privileges from Windows kernel memory.

The steps below focus on after the trigger of the vulnerability, specifically looking at the ROP (Return oriented programming) chain and shellcode.

1. Following the vulnerability trigger, the attacker gains read and write primitives within the Escript.api library (the ability to write and read from memory within the JavaScript interpreter).
2. The attacker redirects the flow of the application by manipulating an object that is pointed from within the leaked Escript.api. The object's execute function pointer is overwritten through a series of steps, so that when the object.execute function is triggered, the first ROP gadget is executed instead. The ROP chain of executable gadgets is needed to transfer execution to the main shellcode.
3. The first ROP gadget to execute is a simple stack pivoting gadget, which in turn points to a second stack pivoting redirection. The second ROP gadget redirects to an array of ROP gadgets, which becomes the new stack. Eventually the ROP chain redirects to the attack shellcode.
4. The shellcode performs reflective DLL loading to map the DLL into memory. This technique is frequently used in advanced attacks to remain in memory and evade detection. This launches the loaded Win32k Exploitation of Privilege exploit.
5. Upon successful exploitation, a .vbs file that can download additional payloads is dropped in the Startup folder.

Overview of the Exploit Process



VBScript CVE-2018-8174 aka “Double Kill”

At the beginning of Q2, a wave of attacks exploiting a new VBScript zero-day dubbed “Double Kill” hit target organizations in China. The vulnerability, CVE-2018-8174, is another great example of a use-after-free (UAF) memory vulnerability with an added twist. Ordinarily, Visual Basic vulnerabilities can only be utilized inside the Internet Explorer browser, limiting their scope and effectiveness. Double Kill, however, uses a technique (URL Moniker) that automatically triggers the Visual Basic exploit directly from an Office document using the IE engine, regardless of whether or not IE is set as the default browser. This means it can be ported both to spear-phishing campaigns and drive-by campaigns to reach a much wider audience of targets and essentially opens the door to an entirely new attack vector.

Potential Impact

This vulnerability has set new records in terms of migration from targeted 0-day attack to criminal mass market exploit kit. Attacks in the wild were first discovered at the end of April. Microsoft released a patch on May 8. It was integrated into the Metasploit framework less than two weeks later and within two days was incorporated into the RIG exploit kit. It's also been added to ThreadKit, Magnitude, GrandSoft, Fallout and other exploit packages. Any unpatched Windows system is vulnerable. UAF vulnerabilities are particularly dangerous as they can enable the execution of arbitrary code, or, in some cases full remote code execution. A successful compromise could eventually give attackers control over the entire system.



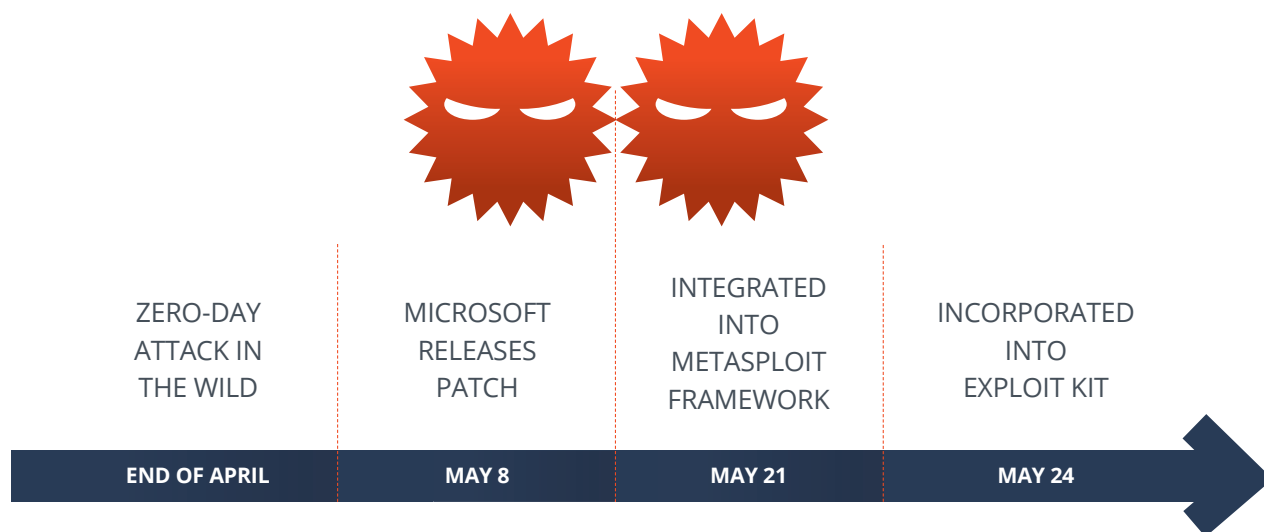
VBScript CVE-2018-8174 aka “Double Kill” (continued)

TECHNICAL DETAILS

The Double Kill attack analyzed here was delivered through a malicious Microsoft Word document with an obfuscated embedded OLE object. The OLE object triggers the download of an HTML page containing VBScript code, which in turn triggers a Use After Free (UAF) vulnerability and executes shellcode. The steps below begin once the victim has opened the Word document.

1. The OLE object contains a URL moniker that connects to and activates the engine behind Internet Explorer to load a remote webpage. The HTML page contains VBScript with obfuscated function names and integer values.
2. The exploit starts by defining a VBScript class object with a class terminate callback, and allocating an array where the first element is the defined class object. Additional VBScript objects are created that point to the created array. The memory is freed by erasing the array which activates the callback. A reference to the freed object gives a UAF vulnerability.
3. The vulnerability allows the attacker to point instead to a new allocated array object that is able to perform arbitrary address reading and writing.
4. The attack uses this functionality to obtain key DLL base addresses. With this information, it then performs operations to bypass DEP and execute shellcode in-memory.
5. In addition to a PowerShell payload, it also runs rundll32.exe to execute another backdoor locally.

Double Kill set new records in terms of migration from targeted 0-day attack to criminal mass market exploit kit.



Mylobot

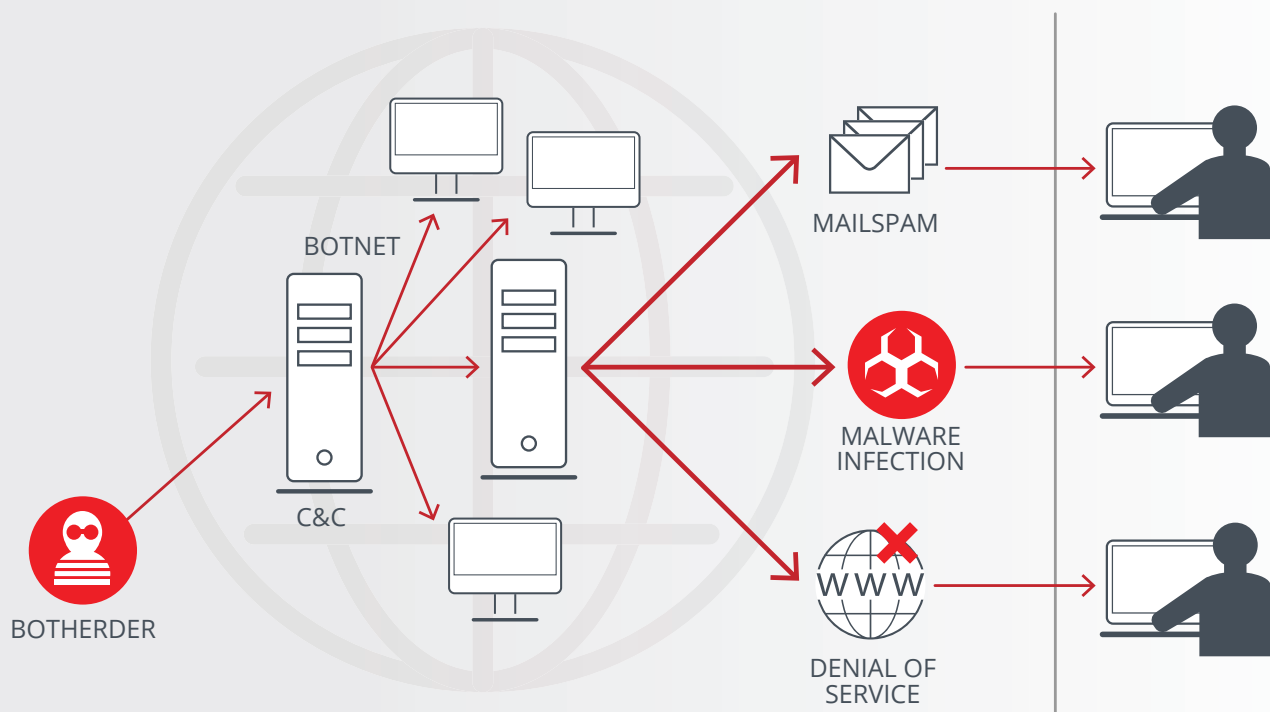
Mylobot is a fairly sophisticated botnet that uses multiple layers of nested files and numerous evasion techniques to avoid detection by security systems. Everything on the victim's end takes place in memory, making it even harder to detect and trace.

One of the more interesting techniques Mylobot includes is the ability to kill other malware by deleting it from the Application Data folder and searching for folders of other botnets. It also disables Windows Defender and Windows Updates and blocks ports on the Firewall.

Potential Impact

Mylobot uses a number of techniques to gain a foothold and evade detection. It gives attackers full control of an infected machine, and ultimately can be used to download any payload, such as banking Trojans, keyloggers, ransomware and distributed denial of service (DDoS), and/or delete and modify files or exfiltrate data to move laterally across a network.

Anatomy of a Botnet



Mylobot (continued)

TECHNICAL DETAILS

Mylobot employs an unusually complex chain attack and combines multiple anti-analysis and evasion techniques that make it more difficult to detect the payload and harder to analyze by security researchers. Some of the threat's core capabilities:

1. Various methods to identify tools used by analysts and virtual machine or sandbox environments. If any of these anti-VM or anti-sandbox checks is positive, then the attack terminates and the end malware payload does not get downloaded on the system, shielding it from automated analysis and detection.
2. It takes out several first line system defenses, disabling Windows Defender and Windows Updates and blocking firewall ports.
3. It checks for other malware running on the system and terminates and deletes it.
4. Mylobot iterates through the PEB (Process Environment Block) to find the addresses for specific, useful functions. It also uses run keys to establish persistence.
5. A delay mechanism postpones access to command and control servers for 14 days. With no immediate network activity or suspicious actions, endpoint detection and response, threat hunting and sandboxing solutions are much less likely to detect the threat.
6. Performs code injection and process hollowing, hiding the code behind a legitimate process to make it harder to detect by security products. It uses CreateProcess to create a process in a suspended state; unmaps the executable memory; then replaces it with the malicious code.
7. Mylobot also employs a fairly uncommon type of reflective loading, where the malicious executable is written directly into memory rather than to a file on a hard drive.

SharpShooter Attack

Penetration testing tools simulate real-world attack scenarios to discover and exploit security gaps. They are essential for security experts to test an organization's defenses and uncover vulnerabilities. They also are a favorite tool of attackers.

Sharpshooter was developed by UK pen-testing firm MDSec for internal use but made publicly available in April, 2018. It incorporates a full fileless delivery mode that operates completely within process memory and has been quickly adopted by malicious actors. SharpShooter is regularly updated by its creators and includes many evasion techniques.

Potential Impact

Fileless attacks that leverage penetration testing tools are increasing, with SharpShooter just one example. New attack framework tools continue to enter the scene, making it easier for non-expert attackers to develop evasive, fileless attacks. The use of these tools combined with other evasive tricks makes detection very hard, allowing them to bypass most security solutions. They also tend to be well maintained, with constant updates and improvements that make them an ongoing threat.

TECHNICAL DETAILS

SharpShooter is a payload creation framework for the retrieval and execution of arbitrary CSharp source code. It creates payloads in a variety of formats, including HTA, JS, VBS, JSE, VBA, VBE and WSF, and embeds them in a template html, which is delivered to the end user using social engineering techniques, with a link through email pointing to a delivery site, or just the archived JavaScript sent directly as an email attachment. SharpShooter features multiple techniques to avoid detection:

1. Identifies tools used by analysts or sandbox environments. These include domain checks, checks for sandbox artifacts, identifying if the execution environment is virtualized and checks for debugging. If any are identified, then the attack aborts before it can be detected.
2. **Stageless Execution** — SharpShooter supports both staged and stageless payload execution. In order to support full fileless mode, the framework provides the ability to inject an in-memory shellcode directly into the process. The shellcode is added to the script file and executed in memory by the serialized .net created payload.
3. SharpShooter supports various script execution methods including SquiblyTwo attacks. SquiblyTwo executes XSL (eXtensible Stylesheet Language) scripts in full trust from Windows Management Instrumentation Command (WMIC) using one of two techniques:
 - One-liners using a COM interface (COM Staging).
 - XSL Exploitation directly through COM: The benefit for attackers of this technique is that it eliminates the risk of being detected through command-line logging.
4. **AMSI Bypass** — Microsoft created AMSI signatures for SharpShooter as well as the DotNetToJavaScript tool used by SharpShooter, which allowed Windows 10 AMSI to temporarily detect SharpShooter attacks. The latest version uses XPath expression on the XSL file to bypass AMSI signatures.

Cobalt Group 2.0

Over the past year, Morphisec and several other endpoint protection companies have been tracking a resurgence in activity from the Cobalt Group. Cobalt is one of the most notorious cybercrime operations, with attacks against more than 100 banks across 40 countries attributed to the group. The most recent attacks show distinct differences, with a subset exhibiting much more advanced functionality. Morphisec Labs believes that the Cobalt Group split following the arrest of one of its top leaders in Spain in March of 2018, with the subgroup we are calling Cobalt 2.0 using more sophisticated delivery methods and other techniques to avoid detection.

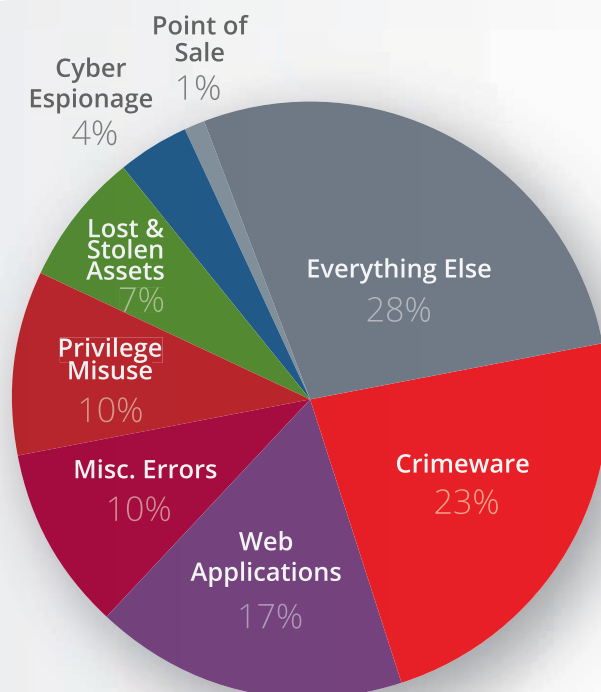
Potential Impact

Threat groups such as Cobalt are increasingly incorporating delivery techniques that allow them to easily bypass whitelisting and AppLocker policies, and we see more and more attacks using legitimate processes to carry out their malicious intent. Although some of the decrypted artifacts used in these attacks have been seen in the wild since the beginning of the year (or earlier), they still are effective as many security solutions cannot detect the artifacts once they are obfuscated and encrypted. Organizations should expect to see much more coming from all Cobalt Group factions during the next year.

FINANCIAL VECTORS OF ATTACK

Crimeware is the top infection pattern for financial institutions, after excluding DDoS attacks and ATM skimmers.

SOURCE: VERIZON 2018 DATA BREACH INVESTIGATIONS REPORT



COBALT GROUP 2.0 (continued)

TECHNICAL DETAILS

As with many other campaigns, the attack begins with a malicious document sent as an email attachment.

1. The weaponized Word document contains a malicious Visual Basic macro. The code is heavily obfuscated and is automatically executed using the `Frame1_Layout` function, which is less likely to trigger security detection than the more widely used `Document_Open` or `AutoOpen` functions.
2. The macro uses the legitimate Windows process `cmdstp.exe` to execute a JavaScript scriptlet (XML with JS) that is downloaded from a malicious website. This limits the exposure and the delivery of the scriptlet to relevant targets only.
3. The JavaScript is encrypted using RC4 and has other custom modifications to avoid detection. It bypasses whitelisting by manipulating `regsvr32.exe`, another legitimate Windows process. The scriptlet drops two artifacts, the payload DLL and a Word document to serve as a decoy replacement for the original weaponized document.
4. The dropped DLL is actually a legitimate PureBasic application with malicious inserted code. PureBasic is a full programming language with numerous possibilities for manipulating the memory.
 - The malicious injected code is reflectively loaded and mapped to existing core functions.
 - It applies anti-disassembly and anti-debugging techniques, obtains several functions from `Kernel32` and `Advapi32`, and uses the identified functions to manipulate the registry to add persistency and next stage identifiers.
- The DLL writes a JavaScript scriptlet into the Roaming directory and then executes `CreateProcess` on the `regsvr32` to download the next stage JavaScript downloader.
5. The JavaScript downloader is obfuscated similar to the first scriptlet. It downloads the next stage JavaScript backdoor using the same `regsvr32` technique to bypass whitelisting used in the previous stage. It also validates the name of the JavaScript backdoor against the name randomly assigned during the previous stage in order to thwart analysis by researchers.
6. The last stage JavaScript (obfuscated in the same way as previous stages) contains backdoor commands that will allow attackers to take over an infected system. It attempts to connect to its C&C server and retrieve tasks to carry out, including downloading and executing PE files and scripts, deleting files, and running shell commands. The script also collects and sends back information about the target environment including the stack of security solutions installed on the computer.

In Conclusion

Like the tides, cybercrime groups and cyber threat trends rise and fall and rise again. From the data and intelligence gathered for this report, some discernible patterns emerge that will affect the threat landscape over the coming months.

FIN7 has made a swift comeback after the arrest of top leaders earlier this year. Expect to see a resurgence in attacks from this cybercrime group, using increasingly sophisticated threats and varying distribution methods.

The banking trojan threat will only grow as cybercrime groups realize that coin miners bring in a tidy sum, but will never be their biggest revenue source. In particular, we see Emotet delivering Trickbot once again rising to prominence as it incorporates more advanced attack patterns and longer attack chains, allowing it to bypass security defenses.

In fact, we anticipate an upswing in trojans of all types — especially remote access trojans, downloaders and infostealers. In addition, the impact of adware will become progressively difficult to ignore as they are leveraged to deliver coin miner and other malware payloads.

Of course, sometimes the only thing consistent about cyber threats is their unpredictability, especially when it comes to APT groups and nation-sponsored attacks. A new zero-day is unleashed and within days becomes a main delivery vector for advanced malware, as happened with the latest Adobe Flash exploits.

A reminder: Morphisec's unique position in the cybersecurity technology space — preventing advanced attacks not caught by standard or next-generation antivirus — makes this threat report different from other industry reports. It brings a perspective beyond sheer numbers for a deeper understanding of the threats that pose the most danger to organizations.



— **Michael Gorelik**, *Chief Technology Officer and Head of Threat Research and the Morphisec Labs Team*

ABOUT MORPHISEC LABS

Morphisec Labs' Threat Research Team engages in ongoing cooperation with leading researchers across the cybersecurity spectrum. The team works closely with counterparts at security, technology and networking companies as well as Fortune 500 security teams, developers of pen-testing frameworks and independent researchers. Morphisec Labs is dedicated to fostering strong collaboration, data sharing and offering investigative assistance.

ABOUT MORPHISEC

Morphisec offers an entirely new level of innovation to customers in its Endpoint Threat Prevention product, delivering protection against the most advanced cyberattacks. The company's patented Moving Target Defense technology prevents threats others can't, including APTs, zero-days, ransomware, evasive fileless attacks and web-borne exploits. Morphisec provides a crucial, small-footprint memory-defense layer that easily deploys into a company's existing security infrastructure to form a simple, highly effective, cost-efficient prevention stack that is truly disruptive to today's existing cybersecurity model.