MORPHISEC
Moving Target Defense

Q1 | 2018 MORPHISEC LABS THREAT REPORT

FOREWORD

Adrian Asher, CISO, London Stock Exchange

There's a continuous battle back and forth between those who defend businesses, and those who want to disrupt business. Cybersecurity sits squarely in the middle of this battleground, bringing techniques and technologies that serve as an organization's last line of defense against the disruption and damage from highly targeted cyberattacks.

Most enterprise security teams, and approximately 30 – 40% of mid-market companies, are taking a more proactive stance against the threats that matter to them. However, it's challenging to keep up with threats that evolve quickly, especially those that are architected to apply speed to infiltration, and conceal methods of data exfiltration.

As added fuel on the fire, attacks and exploits that have yet to be detected, particularly memory-based attacks, put security teams in a position of weakness, without the means to defend.

As a CISO at a global financial institution, I rely on processes and technology that cut time — the time to identify key threats, the time it takes to prevent a threat, and most importantly, how to verify that a given threat is 100% not a threat any longer. 99% doesn't cut it.

CISOs and their teams need every last piece of intelligence and insight that helps push them ahead of attackers by the highest percentage possible. The Morphisec Labs team is leveraging its highly unique approach to defending businesses, and this first edition of their quarterly threat report should be on the radar of every CISO and SOC team interested in better understanding how specific threats can impact them.

Highly analytical, yet prescriptive research is critical to better understand the threat landscape relevant to your business. This report places a distinct focus on analyzing the advanced, evasive attacks that bypass antivirus. It investigates exploit trends as well as five specific threats defended against, to give teams a fresh perspective on some broad-based threats that could impact hundreds of millions of systems.

CONTENTS

Morphisec Labs

Morphisec is dedicated to protecting customers from the most relevant, dangerous cyber threats. The Morphisec Labs team continuously researches attacks and threats to improve defenses, and to share insight with the broader cyber community. Morphisec Labs has developed this threat report, to be released on a quarterly basis, in order to bring this storehouse of information to organizations and other cybersecurity practitioners.

The Q1 2018 Morphisec Labs Threat Report is based on in-depth investigations conducted by Morphisec researchers and anonymized threat data collected from approximately 750,000 installed Morphisec endpoint agents over the first quarter of 2018 (current installed base at time of publication is one million plus). It includes observations about trends in the wider security landscape together with analyses of the tactics and techniques used by malicious actors.

Overview

The first quarter of 2018 saw a large influx of new cyber threats and vulnerability discoveries, in addition to new variants of old standbys such as Corebot, Gamarue, Emotet and Kovter. We found more sophisticated anti-forensic techniques integrated into the live malware samples as well as advancements in the ability to detect and bypass virtual machine isolation environments and security products.

We also found ample evidence that the cyberattack pipeline is getting more efficient and faster. Sophisticated attack technology moves quickly from nation-states to cyber-criminal groups and filters down to mass-market exploit kits in a matter of days.
Nation-states spend the resources finding zero-days and/or developing new attack techniques to exploit them. The more tech-savvy cybercrime groups reverse-engineer patches or use published analyses to develop their own exploits. From there it's only a small step to adding the vulnerability to exploit kits for use by the mass criminal market. February's critical Adobe Flash vulnerability migrated from political zero-day attack to malspam campaign to exploit kit distribution before the month was out.

In looking at the data collected via Morphisec installed agents, we see that adware remains a widespread, but under-the-radar nuisance, comprising over half of prevented attacks. These adware strains employ sophisticated reflective injection of ad material directly into the memory of the process, bypassing antivirus. If you take out adware, more than one-third of the remaining attacks were pure fileless. Every attack included at least one fileless technique.

Of course we can't talk about the first part of 2018 without mentioning the Meltdown and Spectre CPU flaws. With vendors still scrambling to develop manageable updates, the real takeaway is that the security fallout from software and hardware design choices cannot be predicted, enterprising attackers can turn design features into efficient attack vectors and businesses need to be prepared for the unexpected. With the increased attention to side channel attacks by investigative researchers on all sides, this will only become worse.

Q1 | Key Findings

- All attacks prevented by Morphisec in Q1, including adware, used at least one fileless technique. In looking at non-adware attacks, approximately 36% were pure fileless.

- There's been a significant uptick in Banking Trojan attacks, representing over one-third of all non-adware attacks in Q1, with Emotet the top banking malware.

- Although Q1 saw a decrease in ransomware attacks, ransomware continues to be a significant threat to organizations and new strains are constantly emerging, with some, like GandCrab and Samsam, incorporating fairly sophisticated evasive techniques.

- Malware authors are increasingly adding coin mining features to their attacks, even if coin mining is not the primary goal. Payload delivery methods have become more sophisticated, with CryptoNight the most widely used mining algorithm in Q1.

- While threat attribution can be difficult, it is clear that North Korea has become a major threat player. In addition to the RokRAT and Flash Player zero-day attacks profiled in the next section of this report, various other attacks have been linked to the North Korean government and its affiliates.

Select Attack Profiles

Morphisec Labs analyzed numerous threats over the past quarter. 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.

Following are brief profiles of select threats. While they fall across the spectrum of threat type — from ransomware to banking trojans — they all have in common the use of interesting, advanced evasive tactics that lets them go undetected by security solutions.

GandCrab Ransomware

GandCrab first appeared in January and has spread rapidly, undergoing several iterations since its initial version. The ransomware continues to evolve, with new versions being released as soon as a decryptor is developed. GandCrab was delivered primarily via the RIG and GrandSoft exploit kit. Other distribution mechanisms include the EiTest Hoefler Text Pop-up campaign (compromised websites), and a Necurs botnet-powered malspam campaign.

Potential Impact

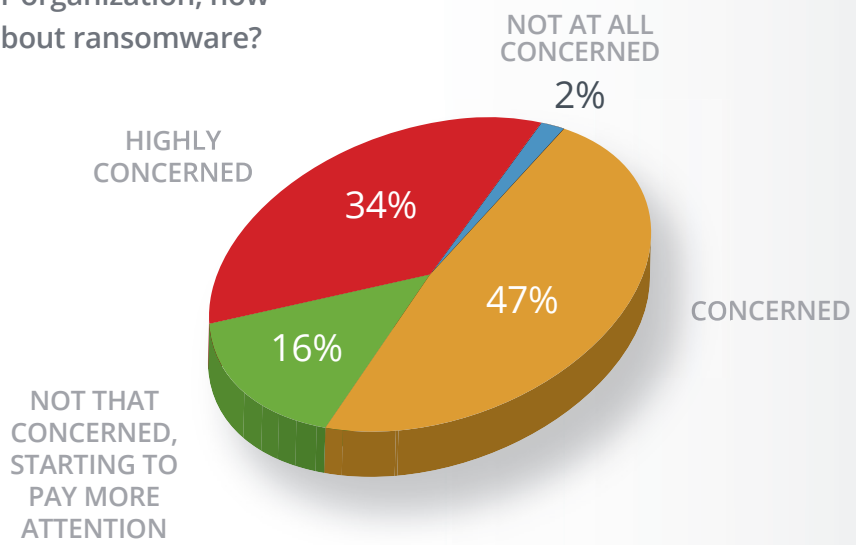
The Russia-based cybercrime group allegedly behind GandCrab uses a partnership "ransomware-as-a-service" approach, focusing its efforts on development rather than running campaigns themselves. It's been estimated that over 50,000 victims were infected by GandCrab by the end of Q1, netting its criminal distributors over $600,000. GandCrab is fast becoming the most active ransomware of 2018.

Ransomware Remains a Top Concern to Organizations in 2018

While coin miners are quickly outstripping ransomware in terms of number of attacks, ransomware is much more destructive for the organization attacked. Executives cite it as a top security concerns for 2018.

In terms of the potential risk to your organization, how concerned is your executive team about ransomware?

(Percent of respondents, N = 651)



Source: ESG Brief: Ransomware: A Priority for 2018.

GandCrab Ransomware (continued)

TECHNICAL DETAILS

GandCrab ransomware is packed by a custom packer, which means it cannot be un-packed automatically by many of the standard tools. The unpacked GandCrab uses multiple techniques to avoid detection, including identifying tools used by analysts or sandbox environments.

1. Queries information about victim OS user, keyboard type, computer name, presence of security solutions, localname, processor type, IP, OS version, disk space, system language, active drives, current Windows version and processor architecture (validates that the keyboard layout is not Russian).
2. Checks against a set of running security solutions processes.
3. Creates a kill list of hardcoded process.
4. Checks connection to command and control server (kill switch) and becomes active only in the event that the C2 server is active. This reduces the footprint and the probability of detection by sandboxes not properly forwarding Internet connection.

It's been estimated that over 50,000 victims were infected by GandCrab by the end of Q1...

Adobe Flash UAF Vulnerability CVE-2018-4878

In early February, the South Korean government warned that an Adobe Flash zero-day was being used in attacks against South Korean targets, most likely by the North Korean government affiliated threat group. This critical vulnerability, CVE-2018-4878, enables remote code execution that can give attackers full control over an affected system. Adobe issued a patched version of Flash player about a week after the zero-day announcement.

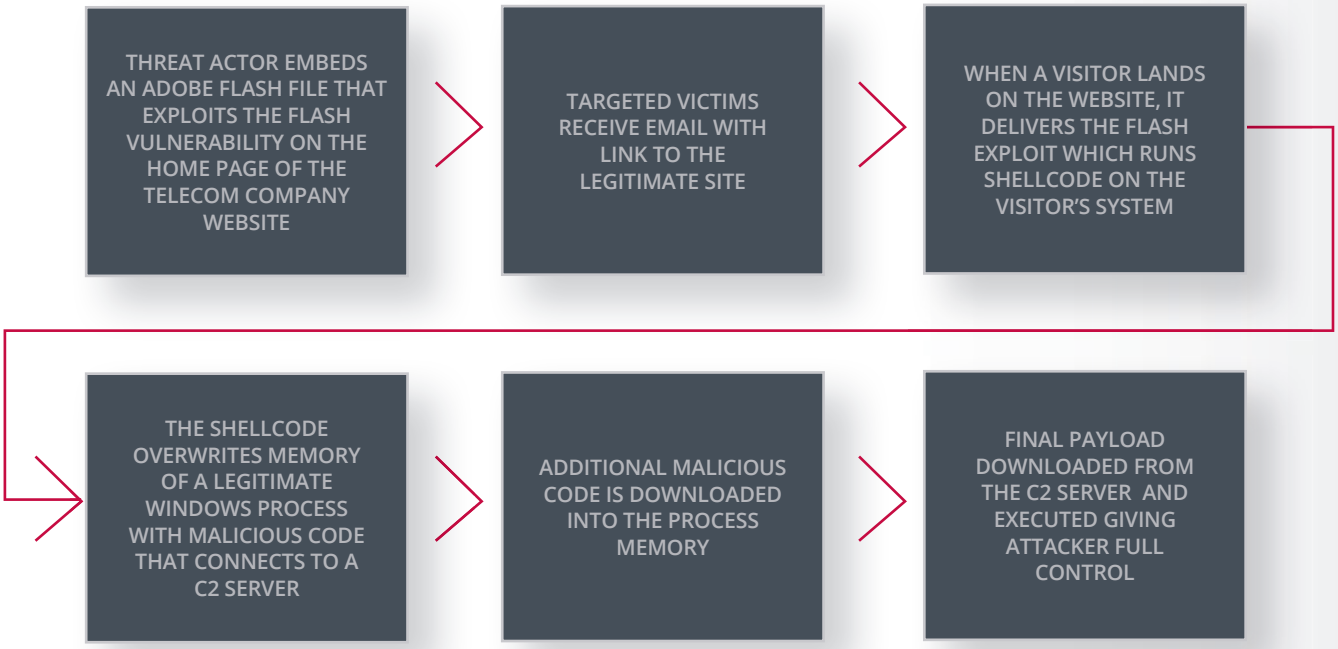
Potential Impact

Given that many still have not patched their systems, this Adobe Flash vulnerability is likely to become one of the most exploited vulnerabilities of 2018.

We can already see signs of this. Two weeks after the patch release, a widespread malicious email campaign exploiting the Flash vulnerability was carried out against U.S. and European organizations. About a week later the vulnerability showed up in the Sundown exploit kit distributing ransomware. And in late March, Morphisec reported that the corporate website of a leading Hong Kong Telecom group was compromised in a watering hole attack that delivers a very similar exploit to the original attack described on the next page.

Anatomy of a Fileless Watering Hole Attack

Only a few weeks after the Adobe Flash zero-day attack, the website of a major Hong Kong Telecom company was hijacked to deliver a watering hole attack exploiting the Flash vulnerability.



Adobe Flash UAF Vulnerability CVE-2018-4878 (continued)

TECHNICAL DETAILS

The malspam attack flow below picks up after the Flash exploit has been delivered by the malicious Word documents which are sent to the targets. It primarily focuses on the 32 bit exploitation flow, although the original exploit supports both 32 and 64 bit applications.

Below is a short summary of the exploit:

1. It starts by initializing the shellcode to a local variable and forwards the flow to the next stage, UAF Triggering.
2. The vulnerability itself is exploited by triggering Use After Free (UAF) on a DRM Operation object. A DRM Listener object is created, the memory freed, and its pointer made to point instead to a new allocated array object created by the attacker.
3. Array Manipulation: The size of the new array is modified to cover the full process virtual memory and a basic validation on the array and the OS is performed.
4. The read primitive and write primitive verifies that the index points to user memory only, to avoid triggering null page guard or kernel memory assets.
5. Now that the exploit gained read and write primitive and is able to fully control the flow, it bypasses DEP by changing the shellcode memory protection to "Execute," and then executing the shellcode in-memory.
6. The attack uses a standard post-exploit technique of using the byte array to locate the different functions.
7. Post Shellcode: CMD.exe is created using the CreateProcessA. Next, to bypass any possible whitelisting solutions, a shellcode is injected directly into the memory of the cmd.exe process by using CreateRemoteThread with a written shellcode inside the process.
8. After additional decryption in CMD.exe process memory, the shellcode downloads and executes malware from the C2 server, in this case a Remote Access Trojan.

ROKRAT

ROKRAT is a Remote Access Trojan (RAT) that first popped up in April 2017 and has been used in various campaigns since. It's interesting to examine as it employs several of the sophisticated evasive techniques we frequently see. It can detect if the targeted system is running any malware detection, debugging tools or is a sandbox environment and take action accordingly. The ROKRAT variant analyzed by Morphisec was delivered via spear phishing email campaigns targeting South Korean politicians and activists. The malicious document leveraged a vulnerability in Hangual Word Processor (HWP). The attack remains unattributed, but the most likely suspect is North Korea (https://blog.talosintelligence.com/2018/01/korea-in-crosshairs.html).

Potential Impact

Once inside, ROKRAT gives attackers nearly unlimited control to kill processes, download and execute additional malware, log keystrokes, capture screenshots and exfiltrate data, including information that could lead to compromises of other systems.

TECHNICAL DETAILS

The infection vector in the attack analyzed is a malicious HWP document containing an embedded Encapsulated PostScript (EPS) object. The EPS object exploits a well-known EPS buffer overflow vulnerability, CVE-2013-0808, and drops a binary disguised as a JPG file.

1. The dropper, packed by a custom packer to evade antivirus, contains a resource named SBS/Doc with malicious shellcode. The dropper creates a new cmd.exe process, injects the extracted resource and executes it.

2. The shellcode decodes an XOR-obfuscated Portable Executable file, loads it to the memory of cmd.exe and executes it. This is the ROKRAT trojan.

3. The payload collects information about the OS and system, performing a number of anti-analysis checks including checking for a sandbox environment. After the checks are complete it initiates Command and Control communication.

4. Many security tools can detect traffic to and from malicious IP addresses. To prevent this, the trojan uses legitimate Mediafire, Yandex, and Twitter cloud platforms for its command and control communications and exfiltration platforms.

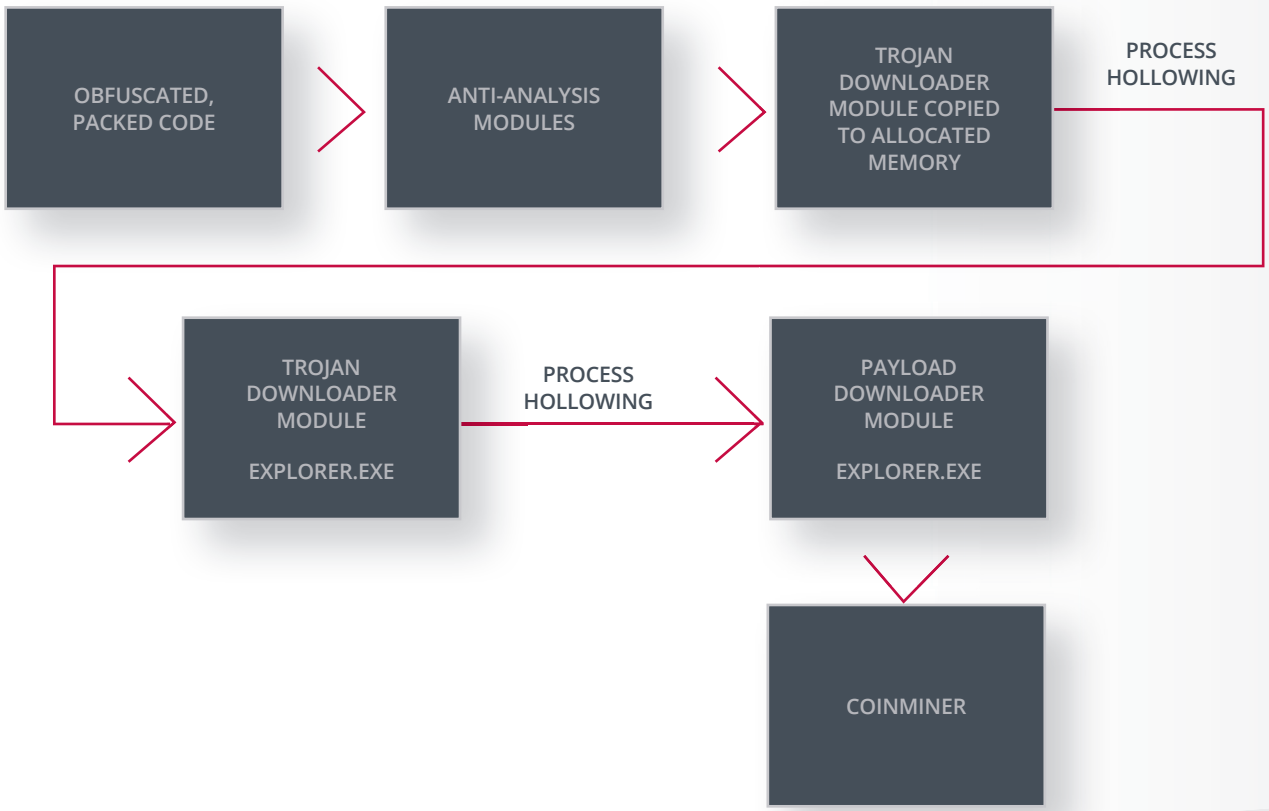
Dofoil/Smoke Loader Trojan with Coinminer

One of the more interesting trends of 2018 is the rapid proliferation of cryptocurrency miners. In early March, a variant of the Dofoil trojan emerged that includes a resource-draining crypto-currency-mining payload. This Dofoil variant used multiple tactics to establish persistence, remain undetected and confound dynamic and static analysis.

Potential Impact

Dofoil attacks have popped up fairly regularly over the past several years, with new tricks added in and delivering various payloads. While this particular Dofoil attack appears to be no longer active, we are currently investigating new Dofoil/Smoke Loader variants, which are even more evasive. In addition, we will certainly see coinminers of the type used in this attack incorporated in other malware.

Dofoil Attack Flow



Dofoil/Smoke Loader Trojan with Coinminer (continued)

TECHNICAL DETAILS

Like the other attacks we've looked at, the malware delivered is heavily packed and obfuscated.

1. Doifoil uses multistage shellcode incorporating various anti-analysis techniques. It first iterates over the PEB (Process Environment Block) to find modules and functions useful to its evasive tactics.

2. The malware uses VirtualAlloc API to allocate a new memory region and adds offset to the start of the allocated base region.

3. It then copies the decrypted code to the newly allocated memory area.

4. Dofoil then performs Process Hollowing/RunPE injection to hide the code behind a legitimate process so that it is harder to detect:

   - It creates an explorer.exe process in suspended mode.
   - Unmaps (hollows) the original executable from the process.
   - Then replaces it with a malicious Portable Executable (PE) from the allocated memory.
   - The trojan checks to make sure it Is not running in a virtual machine environment. If so, it stops running. If not, the hollowed explorer.exe creates a second hollowed explorer.exe instance.
   - This second explorer.exe drops and executes a Coinminer that uses the name of a legitimate Windows binary, wuauclt.exe. In this case, it mines Electroneum coins but could be configured to mine various other cryptocurrencies.

The cryptocurrency miner itself uses several techniques designed to avoid detection, including checking for analysis tools and stopping them.

Cybercriminals are adding coin mining features to various types of malware, from exploit kits to banking trojans.

DISCOVERED BY
Morphisec Labs
RESPONSIBLY DISCLOSED
TO MICROSOFT

CIGSlip

CIGSlip is not an attack but a security flaw discovered by Morphisec researchers, which can be exploited by attackers to bypass Microsoft's Code Integrity Guard (CIG). CIG is a feature that prevents malware from loading malicious "unsigned" code into applications such as Microsoft Edge. A CIG-protected application will load only Microsoft-signed DLLs and binaries. However, using CIGSlip, attackers can easily load malicious libraries into CIG-protected processes and applications by exploiting a loophole in the handling of non-CIG-enabled process.

Potential Impact

CIGSlip carries serious destructive potential and organizations should understand the possible damage that could be inflicted through this attack surface. Any Windows machine is at risk. CIGSlip enables attackers to load any DLL (not signed) into a protected CIG process without triggering an alert notification. This means, for example, that a banking trojan could load malicious plugin into the Edge browser.

TECHNICAL DETAILS

It is a known fact that attackers can create a Non-CIG malware process or inject their malicious code into already running, existing Non-CIG critical process (e.g. explorer.exe). Non-CIG-protected processes are the most prevalent form of process on Windows and there is no feasible way to protect all processes with CIG as programs such as Outlook, for example, with all its 3rd party add-ins, could not load. From within the compromised Non-CIG process, attackers can then apply CIGSlip to compromise a CIG protected process.

CIGSlip leverages the fact that a process can load a binary constructed from a section that could be injected from outside. This will bypass the verification check for the DLL signature that is done during sectioncreate CIGSlip detours the code integrity verification by hijacking control when the section is created, eventually enabling injection of the malicious DLL. A detailed proof-of-concept can be found in our CIGslip report https://blog.morphisec.com/new-method-to-bypass-microsoft-cig

In Conclusion

The first quarter of 2018 serves as both a good indicator for the year ahead and a caution that just when we think we understand the cybersecurity landscape, a seismic shift can alter it completely.

Of course some things never change. Cybercriminals are always looking for the low hanging fruit, the easiest ways to make money. Coinminers, which generate immediate, certain revenue and can operate undetected longer, are edging out ransomware as the preferred payload delivered by many malware downloaders.

The greatest sources of cybercrime revenue, however, remain Information stealers and Banking trojans. These saw a resurgence in Q1, albeit with significant upgrades, thanks to the availability of more advanced techniques to hide malware and evade security solutions, particularly fileless tactics. Attackers have increased their distribution of very sophisticated Banking trojans like Emotet, Corebot, Zeus Panda across a broader attack surface.

Some trends emerging will only manifest as organizational threats later. Many researchers, on both sides of the aisle, are now investigating side channel attacks due to the attention generated by Meltdown and Spectre and their destructive potential. We anticipate additional side channel attack research will be published during the year, although those attacks will be more theoretical than practical.

A more immediate upcoming threat are Use-After-Free memory exploits, such as the Adobe Flash vulnerability CVE-2018-4878 analyzed in this report. Although there are many vulnerabilities, only a few of them can really be weaponized. Use-After-Free exploits are easily weaponizable and we expect to see such memory exploits become a main vector to deliver sophisticated fileless attacks.

One final note: The data and analyses in this threat report are different from other industry reports as, like Morphisec, it focuses on attacks not caught by antivirus or antivirus replacements. It is intended to offer a perspective that goes beyond sheer numbers to bring deeper understanding of the threats most relevant and dangerous to organizations today.

— **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.

MORPHISEC
Moving Target Defense

www.morphisec.com