ALERT LOGIC®

TOP 5 MALWARE TRENDS

Find out how attackers are accessing systems and how to stop them

Security has always been a fast-paced field, but lately the pace has been accelerating. Malware is rapidly evolving. The ways payloads are being delivered and deployed are changing, too. New attack tools and exploit techniques are appearing more regularly. It's taking less time for them to gain widespread adoption. For all of those reasons, we thought it would be valuable to share additional insight into the threatscape we shared in the 2018 Critical Watch Report.

At that point, the industry was still reeling from the WannaCry and NotPetya outbreaks. Elements of those two attacks can be found in many of today's threats, and our prediction that they would strongly influence how many future attacks operate continues to prove out. We also shared thoughts around the drop-off in ransomware and the rapid rise of cryptomining malware in its place. That switch in payloads was also emblematic of a larger, more fundamental shift in attack priorities — with ransomware in sharp decline, malware authors are once again designing for stealth. That means leaving lighter footprints, and in an increasing number of cases, attacks are being adapted to no longer save executables to disk at all. With those important changes in mind, we'd like to share insights into the ways malware is evolving. In doing so, we can see that five key trends emerge:

1. The wider adoption of fileless attack techniques designed to bypass traditional security solutions like antivirus.
2. A rise in clickless infection driven primarily by the use of remote execution exploits (like EternalBlue) and RDP brute force attacks.
3. The increased practice of living off the land — avoiding detection by abusing legitimate system tools and processes rather than dropping malicious files on disk.
4. The resurgence of worm capabilities designed to help infections spread further, faster.
5. A shift away from ransomware in favor of cryptomining payloads, instead.

Lastly, we will cover how partnering with a company like Alert Logic can assist you will implementing a security solution that will advance your capabilities far faster than you can achieve on your own. By partnering with a managed security provider, organizations gain access to a modern, always-advancing set of technology to help secure their business, the intelligence to provide context to security decisions, and expertise and remediation guidance to help secure their business.

TREND #1: FILELESS ATTACK TECHNIQUES

It's never been easier to infect systems silently, without downloading malicious programs or leaving behind any obvious trace.

WHAT WE'RE SEEING

More attacks avoiding the use of malicious executable files in favor of using exploits, scripts, and legitimate system tools, instead.

WHY IT'S HAPPENING

By not installing malicious files, attackers are able to bypass traditional and next-generation antivirus solutions that rely primarily on file scanning.

EXAMPLES

Attacks that abuse scripting languages like PowerShell and VBScript, attacks that use or code injection techniques or exploits to load and execute malicious code directly in memory, attacks that create or make changes to registry entries, etc.

WHAT'S NEXT

Watch for fileless techniques to gain even wider adoption as more criminals adopt red team tools and penetration testing frameworks.

WHAT TO DO NOW

Disable or restrict powerful administration tools like PowerShell, practice the principle of least privilege, and utilize endpoint security that blocks malicious activity, not just file signatures.

> *"A THIRD OF ALL ATTACKS ARE PROJECTED TO UTILIZE FILELESS TECHNIQUES IN 2018. "*
> - THE PONEMON INSTITUTE

TREND #2: CLICKLESS INFECTION

End users have long been blamed as the weakest link in security. But many of the latest attacks are bypassing user interaction altogether.

WHAT WE'RE SEEING

A growing number of attacks that don't rely on tricking users and instead take a more direct path to launching successful infections.

WHY IT'S HAPPENING

The release and proven effectiveness of the EternalBlue exploit has played a big part, but bypassing users also simply allows attackers to infect machines more efficiently and reduce their chances of detection.

EXAMPLES

Attacks leveraging the EternalBlue exploit (WannaCry, NotPetya); RDP brute force attacks (Samsam, CrySiS, Shade). WHAT'S NEXT Be on the lookout for more WannaCry-like attacks, this time exploiting Remote Desktop Protocol (RDP) or other vulnerabilities.

WHAT TO DO NOW

Secure or disable SMB and RDP, patch what you can and isolate what you can't, and deploy endpoint security with exploit and behavioral-based protection.

"IN Q2 2017, ONE RDP BRUTE FORCE ATTACK COST A BUFFALO, NY HOSPITAL $10,000,000."

- THE BUFFALO NEWS

TREND #3: LIVING OFF THE LAND

To gain access and persistence, attackers are increasingly using an organization's own system tools and processes against it.

WHAT WE'RE SEEING

Increasing cases of attackers abusing legitimate tools already present on the system rather than dropping malicious files on disk.

WHY IT'S HAPPENING

Leveraging system tools and avoiding the use of malware executables is making these attacks extremely difficult for traditional security to detect.

EXAMPLES

Attacks utilizing macros, PowerShell scripts, and tools like PsExec and wmic.

WHAT'S NEXT

Expect use of living off the land and fileless attack techniques to continue to grow from being exceptions to being the norm.

WHAT TO DO NOW

Disable tools and commands you don't actively need, and make sure your endpoint security doesn't just rely on file scanning or whitelisting, which these attacks can bypass.

"A GOOD HACKER AVOIDS THE USE OF MALWARE AND CODE EXPLOITS WHENEVER POSSIBLE.... THERE'S NO SENSE IN USING MALICIOUS CODE WHEN SIMPLER AND QUIETER MEANS ARE AVAILABLE."

- LESLEY CARHART

ATTACKER GOALS	LEGITIMATE SYSTEM TOOLS
Initial Infection	Macros, PowerShell, VBScript, RDP
Credential Harvesting	Mimikatz, Windows Credentials Editor (WCE), pwdump
Lateral Movement	PsExec, Windows Management Instrumentation (WMI), RDP2
Persistence	WMI, Group Policy Objects (GPOs), Scheduled Tasks

TREND #4: WORM CAPABILITIES

We're seeing more and more attacks taking a self-spreading, land-and-expand approach so they can infect as many machines in as little time as possible.

WHAT WE'RE SEEING

More attacks with built-in worm components designed to make infections selfspreading and more difficult to remove.

WHY IT'S HAPPENING

The success of WannaCry and NotPetya has inspired attackers to revisit worms to propagate their infections more rapidly.

EXAMPLES

WannaCry and NotPetya; Emotet, QakBot, and TrickBot banking trojans.

WHAT'S NEXT

Watch for worm modules to become commoditized, purchasable add-ons for a variety of malware.

WHAT TO DO NOW

Prioritize security that can block these attacks in realtime, before infections have the chance to spread and get entrenched.

TREND #5: CRYPTOMINING

Cryptominers — malware designed to hijack a victim's CPU or GPU power to mine cryptocurrency without their knowledge — are the new top attack payload of choice.

WHAT WE'RE SEEING

Attackers are abandoning ransomware in droves and deploying cryptomining payloads, instead.

WHY IT'S HAPPENING

With fewer victims paying ransoms, installing cryptomining malware on compromised machines has emerged as a stealthier, more direct source of revenue.

EXAMPLES

Wannamine (named after WannaCry thanks to its use of EternalBlue to spread), Smominru botnet of 500,000 infected computers, attacks targeting specific vulnerabilities (ex: Jenkins Miner), etc.

WHAT'S NEXT

Expect to see more and more malware treating cryptominers as "why not?" attack add-ons to be deployed alongside credential stealers, backdoors, and other payloads built for persistence and stealth.

WHAT TO DO NOW

The shift from ransomware to cryptominers means infections are no longer clearly noticeable. Worse, the presence of cryptominers is indicative of other malware hiding around. To prevent these silent attacks from taking hold, organizations need to prioritize preventative measures like replacing legacy antivirus solutions with stronger, more modern endpoint protection, instead.

\These latest trends in malware aren't just raising the stakes, they're also placing new demands on security. To protect your organization, you need to make sure you can:

- **Gain visibility into your environment** to understand your risks and begin to reduce your attack footprint.
- **Detect and block fileless techniques:** When attacks avoid dropping malicious files traditional security solutions aren't enough. Stopping them requires stronger, more modern protection from exploits and scripts, plus greater visibility into system activity.
- **Prevent clickless infection:** When attacks skirt traditional infection vectors like email and compromised websites protection can't just be focused on the network level, it needs to be focused on company endpoints, as well.
- **Respond to attacks attempting to live off the land:** When attacks use legitimate system tools rather than malicious files protection can't be limited to file scanning and whitelisting.
- **Preemptively block worming capabilities:** When all it takes is one infected computer to compromise an entire network it's vital to block any attacks that land on an endpoint at the very outset.
- **Stop cryptomining and other attacks designed for stealth:** When malware is designed to run silently in the background, relying solely on detection and response tools isn't a viable option.

You need tools that can prevent successful compromise in the first place and a security partner to provide help if you need it. Find out how Alert Logic helps companies meet all five of these demands by blocking exploits, fileless, and file-based attacks before they cause any damage. In addition, Alert Logic delivers an award-winning solution with visibility, vulnerability assessment, threat detection and response, and web application security to provide the right level of coverage at the right cost. Our SIEMless approach protects public cloud infrastructures, container workloads, as well as traditional data-centers and endpoints.

ALERT LOGIC®