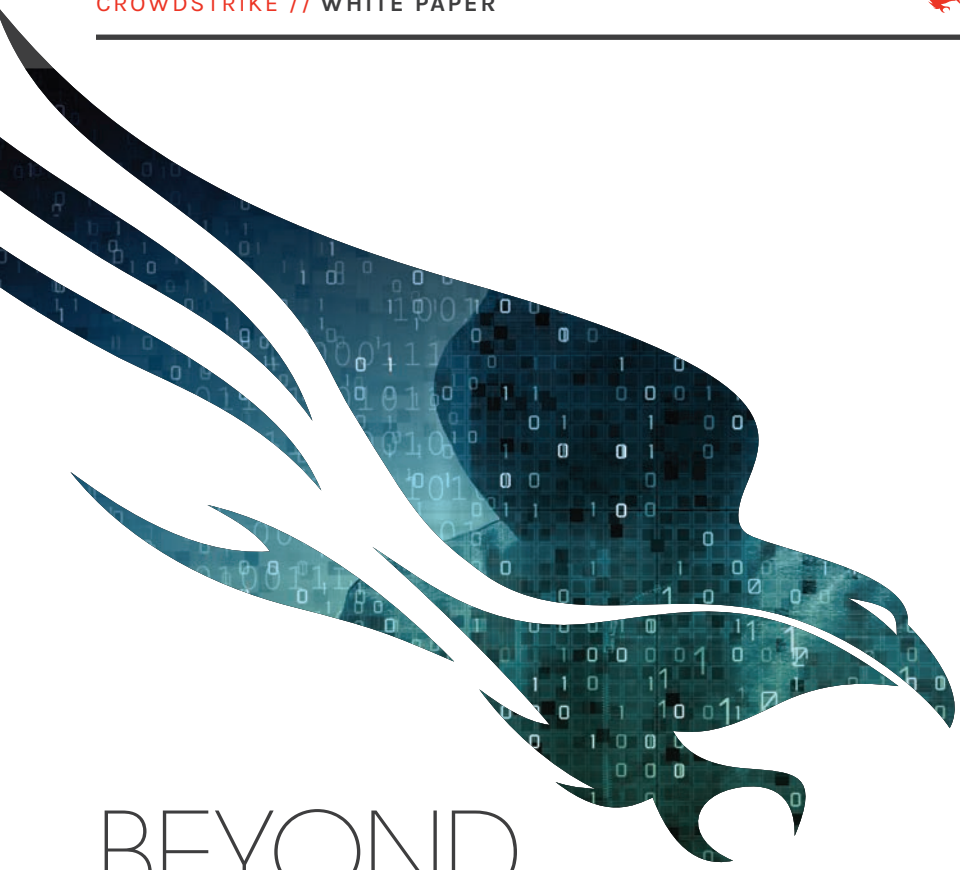


BEYOND MALWARE: DETECTING the UNDETECTABLE

How to Detect and Respond to Malware-Free Intrusions

MOST ORGANIZATIONS TODAY FOCUS ON PROTECTING THEIR NETWORKS AGAINST MALWARE, EXPLOITS, MALICIOUS WEBSITES, AND UNPATCHED VULNERABILITIES. UNFORTUNATELY, THERE IS A FUNDAMENTAL FLAW WITH THIS APPROACH:

A MALWARE-CENTRIC DEFENSE APPROACH WILL LEAVE YOU VULNERABLE TO ATTACKS THAT DON'T LEVERAGE MALWARE.

A malware-centric strategy is too simplistic to provide an adequate defense against today's sophisticated adversaries.

HERE'S WHY: Malware is responsible for only 40 percent of breaches[1], and external attackers are increasingly leveraging malware-free intrusion approaches to blend in and "fly under the radar" by assuming insider credentials within victim organizations. The nature of the game now is persistence and gaining long-term access to the enterprise. The chances of ultimate discovery and effective remediation diminish greatly when no external binaries are brought into the environment and no unusual outbound C2 (command and control) traffic is taking place.

The idea behind a malware-free intrusion is very simple — malware, even if it's unknown to AV, is still very noisy. The presence of unknown and previously unseen binaries running in your environment; making file and registry changes to your system; and calling out to the network — these are all things that can be observed and trigger eventual suspicion on the part of a proactive SOC (security operations center) analyst or incident responder. So if you're an attacker who's trying to stay undetected for as long as possible, what do you do?

The obvious answer is that you break in without using malware, emulating legitimate insiders. Insider detection has always been one of the hardest problems to solve in cybersecurity because the attacker, by definition, looks like someone who is supposed to be inside your network and doing things that are largely legitimate and expected. Thus, if the adversaries can emulate this behavior, they achieve their objective of stealth.

MALWARE-FREE INTRUSION: SEEN IN THE WILD.

A large defense contractor hired CrowdStrike Services after struggling for months to remediate an intrusion from a sophisticated nation-state affiliated actor. The adversary kept coming back and the client could not identify the point of entry, despite having numerous host and network forensics, whitelisting, as well as Indicator of Compromise (IOC)-scanning malware detection tools.

The explicit mission was to identify the C2 channels the adversary was using to get back inside the environment. In the end, it turned out that the question they were posing — identification of the C2 servers — was the wrong one. Once the services team deployed next-generation endpoint technology across their servers and desktops to profile and identify all adversary activity, it was determined that the adversary had compromised their two-factor authentication system, stolen the seed values and was coming in through the VPN system using

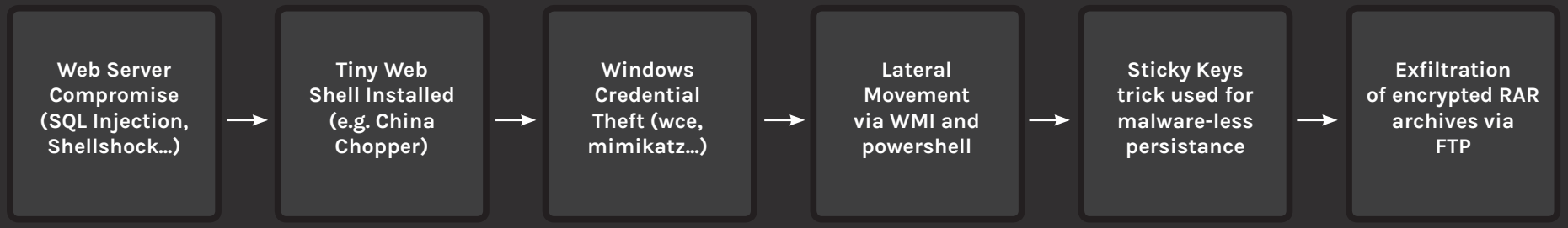
1 According to Verizon's Data Breach Investigations Report (DBIR)

legitimate credentials and generated two-factor token values. There were no C2 server IOCs to detect, and once the adversary was inside the network, they were able to move around using legitimate credentials and windows system administration tools, without the actual use of malware.

This critical gap between current enterprise defense strategy and the evolution in adversary tactics is responsible for a growing number of successful intrusions, as well as the fact that a typical breach remains undiscovered for over 200 days. In response, organizations now need to adapt their strategy and augment their malware-detection and IOC scanning tools with solutions that can hunt for, detect, and ultimately prevent adversary activity even when no malware is present.

DIVING DEEPER:
HOW DOES A MALWARE-FREE ATTACK WORK?

Chinese nation-state affiliated actors, such as DEEP PANDA and HURRICANE PANDA, have been observed using the following tradecraft.



MALWARE-FREE INTRUSION TRADECRAFT

The intrusion begins with a compromise of an external-facing web server, often a Windows IIS server. Such compromise can be achieved via SQL injection, WebDAV exploit, or, as we've seen recently from DEEP PANDA in attacks against Linux web servers, the use of the Bash vulnerability known as ShellShock. That allows actors to install a webshell on the server, with China Chopper being the most common tool of choice. The reason it's so popular is that it is almost elegant in its simplicity. The webshell consists of a tiny text file (often as little as 24 bytes in size) that contains little more than an "eval()" statement, which allows the attacker to execute processes on the web server. That script can be obfuscated easily to evade signature and IOC scanning technologies.

CHINA CHOPPER WEBSHELL CONTROLLER

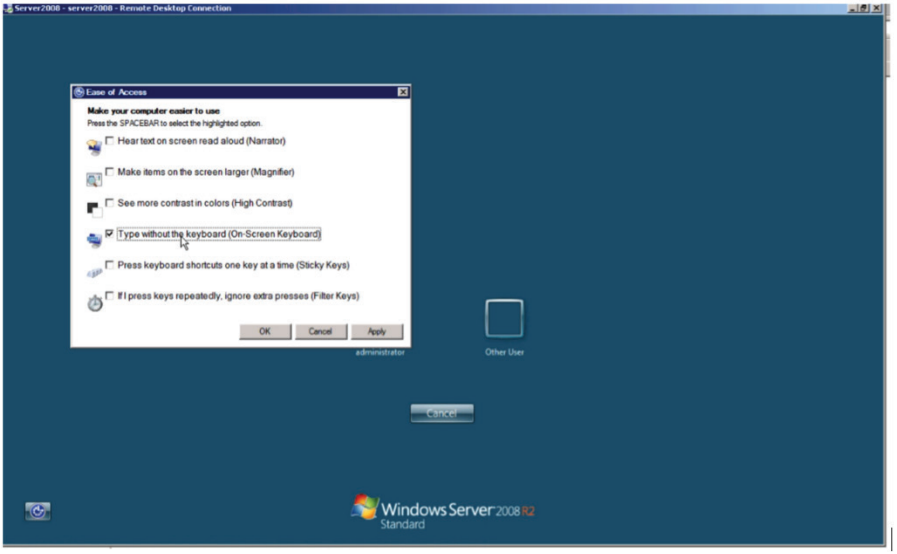
On the attacker's side, they run a controller application (see screenshot above), which allows them to upload/download files and provides access to a virtual terminal to execute commands.

Through that webshell, the adversary then uploads a credential theft tool to steal Windows passwords and hashes, and on occasion, even Kerberos Golden Tickets that can give an adversary persistent access to the network for as long as a decade! (Technically, one might label such a tool as malware, but traditional anti-malware defenses usually will not catch it, as there are numerous repackaged/rewritten versions of these credential theft tools that can escape all signature and IOC-based detections.)

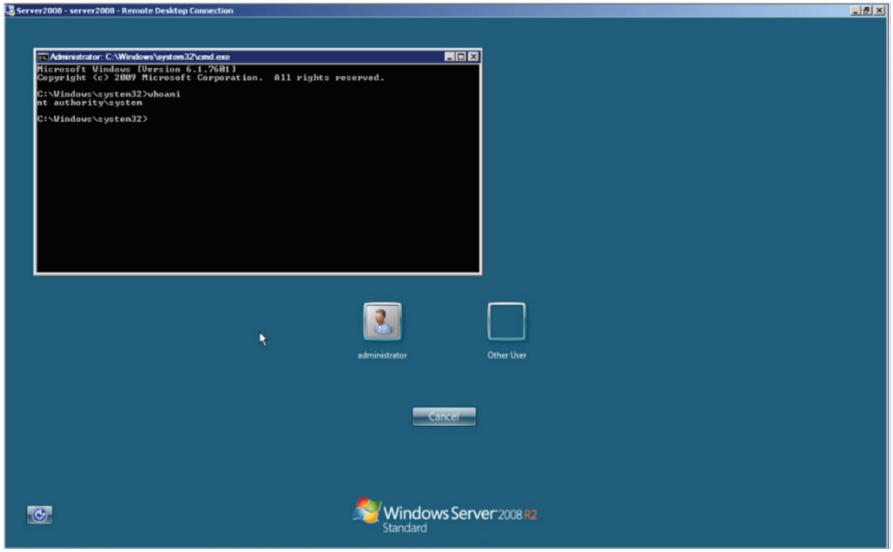
Once credentials are acquired, the adversary will move laterally using WMI commands or RDP sessions, just as a Windows administrator might do, and use scheduled tasks with powershell scripts to maintain persistence.

Frequently, we also see the use of the "sticky keys" trick for maintaining malware-free persistence on a victim network. With this trick, the adversary will modify the registry on a remote machine (typically using WMI) to set "cmd.exe" as a Debugger for tools like sethc.exe (StickyKeys) and osk.exe (On-screen keyboard). Once that's done, an attacker can RDP into that machine and press the StickyKeys or On-Screen Keyboard hotkeys and instantly get a command prompt running with system-level privileges, without even requiring a login to the remote server. Thus, even if passwords are reset across the victim's environment, the adversary may still maintain persistent access unless all the registry entries are cleaned up.

Example command:
wmic /user:<REDACTED> /password:<REDACTED> /
node:<REDACTED> process call create “C:\Windows\system32\
reg.exe add \”HKLM\SOFTWARE\Microsoft\Windows NT\
CurrentVersion\Image File Execution Options\osk.exe\” /v
\”Debugger\” /t REG_SZ /d \”cmd.exe\” /f



On Screen Keyboard triggered from Windows logon prompt



Command prompt running with SYSTEM privileges

Lastly, they will use standard FTP commands to exfiltrate the data out of the environment onto their C2 server, making sure to encrypt it beforehand (usually with RAR archiver) so as to evade network DLP solutions that may look for confidential content leaving the network.

Here is an example of one such attack detected via Falcon, CrowdStrike's next-generation endpoint technology, at a customer location (the specific usernames/machine names have been replaced to protect confidentiality):

ATTACK PROCESS TREE FROM FALCON HOST

As you can see from the full Falcon Host process tree, after initial reconnaissance (whoami/systeminfo/quser), the adversary uploaded and executed a custom-repacked version of Windows Credential Editor. Next, they proceeded to use WMI to edit remote registries for the StickyKeys persistence trick and, afterward, copied files from remote shares via "net use." Finally, they used RAR to encrypt and compress the data to exfiltrate it out of the network (this time, simply downloading it through the webshell).

DETECTING AND PREVENTING MALWARE-FREE INTRUSIONS WITH NEXT-GENERATION ENDPOINT PROTECTION

If your security tool is just setting up a perimeter and trying to fend off malware, then you could have an undetected intruder on your network for weeks, months, or years. These types of attacks have happened in the past, but businesses still seem to miss the point that the threat extends beyond just malware. As we detailed above, theft of data can be accomplished without the use of malware by purely leveraging common and legitimate Windows administrative tools WMI or Powershell scripts.

The opportunity to keep an attacker from doing reconnaissance on your network, stealing credentials, and moving laterally occurs when you can actually detect the breach and stop it before any theft of IP or actual destruction of your network takes place. Unless you have what it takes, in terms of technology and people, to identify breaches within seconds of them occurring – regardless of whether malware is used in the attack -- you will ultimately lose.

Defending against malware-free intrusions requires you to enable next-gen endpoint protection built on three core principles:

100% CLOUD-BASED ARCHITECTURE

- Allow for frictionless deployment of a lightweight, zero-impact sensor to hundreds of thousands of endpoints in minutes
- Provide seamless and continuous detection, prevention, monitoring, and search capabilities
- Correlate billions of events and petabytes of data in real time

INDICATOR OF ATTACK (IOA) APPROACH

- Move from a reactive Indicators of Compromise (IOC) approach to a proactive Indicators of Attack (IOA) detection strategy
- Focus on identifying adversary objectives, as opposed to simply detecting malware tools or the presence of post-breach IOCs
- Allow for IOA detection of attacks in progress, providing the ability to spot an attack prior to a devastating data breach

24/7 VISIBILITY, MONITORING, AND RESPONSE

- Integrate intelligence and expertise to provide context and assigns priority to threat response
- Measure time to response is measured in milliseconds: time to remediation in minutes or hours, not days, weeks, or months
- Prioritize attack indicators instantly

These core areas are no longer just part of an emerging approach but critical building blocks for effective cyber defense. In order to protect against today's advanced attacks, organizations need to implement next-gen security architecture and ask security vendors to prove their effectiveness in detecting adversary activity and the use of malware-free intrusions.

ABOUT CROWDSTRIKE

CrowdStrike™ is a leading provider of next-generation endpoint protection, threat intelligence, and pre- and post incident response services. CrowdStrike Falcon is the first true Software as a Service (SaaS) based platform for next-generation endpoint protection that detects, prevents, and responds to attacks, at any stage - even malware-free intrusions. Falcon's patented lightweight endpoint sensor can be deployed to over 100,000 endpoints in hours providing visibility into billions of events in real-time.

CrowdStrike operates on a highly scalable subscription-based business model that allows customers the flexibility to use CrowdStrike-as-a-Service to multiply their security team's effectiveness and expertise with 24/7 endpoint visibility, monitoring, and response.

Request a demo of CrowdStrike Falcon
and learn how to detect, prevent, and respond to attacks, at any stage - even malware-free intrusions.
http://www.crowdstrike.com/request-a-demo