Malware-Free Intrusions: Adversary Tricks and CrowdStrike Treats »

By Dmitri Alperovitch

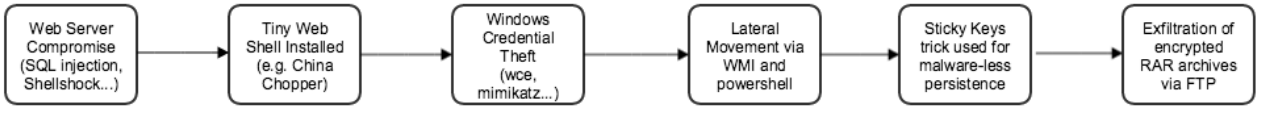
Published: 2014-10-31 · Archived: 2026-04-06 03:34:30 UTC

‘Tis the season for trick-or-treating, so I thought it might be a good time to share some of the new tricks we’re seeing from the land of targeted adversaries in evading existing security defenses and penetrating networks.

One of the key consistent trends that has been observed this year is a move on the part of the more advanced actors to a technique I call “malware-free intrusion.” The idea behind it is very simple — malware, even if it’s unknown to AV, is still very noisy. You have unknown and previously unseen binaries running in your environment; they’re making file and registry changes to your system; calling out to the network — all things that can be observed and trigger eventual suspicion on the part of a proactive SOC 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 and emulate legitimate insiders.

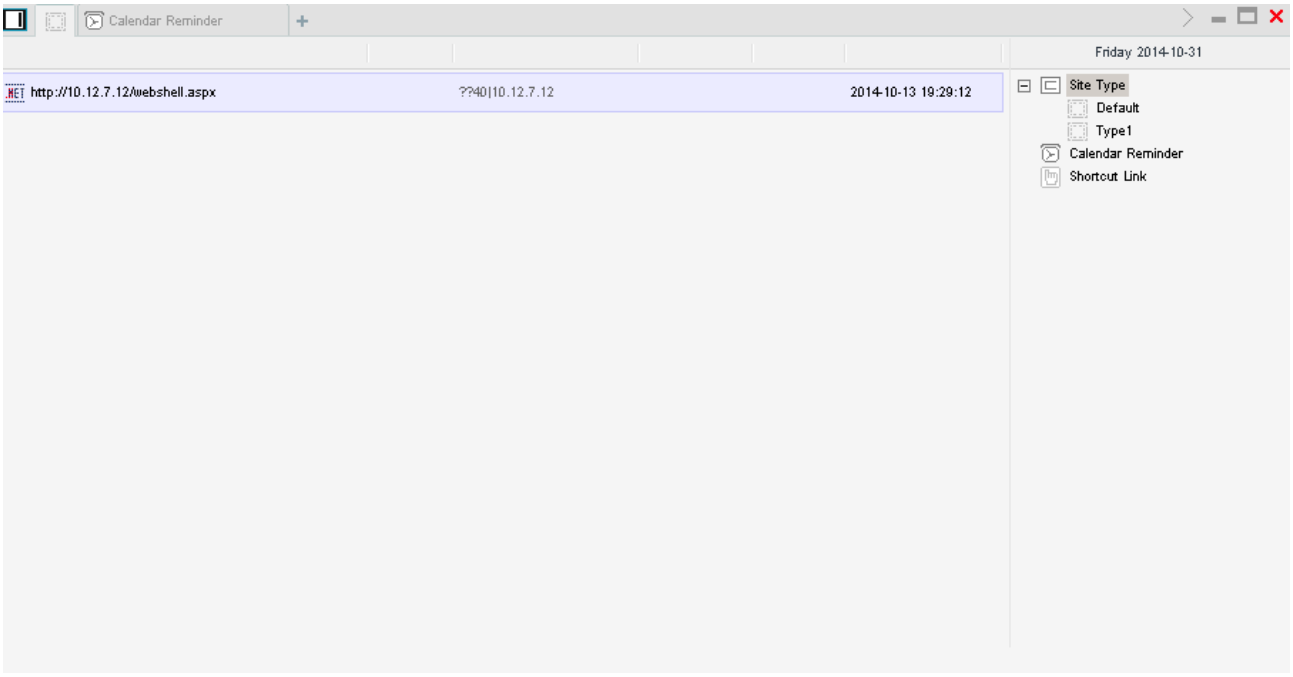
Insider detection has always been one of the hardest problems to solve in cybersecurity because the attacker by definition looks like someone who is supposed to be inside your network and doing things that are largely legitimate and expected. Thus, if the adversaries can emulate this behavior, they achieve their nirvana of stealthiness.

In the last year, we have seen a number of different Chinese nation-state affiliated actors (we track them under cryptonym of“Panda”), such as DEEP PANDA and HURRICANE PANDA, leverage the following interesting 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 recently discovered bash vulnerability (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 beautiful in its simplicity. The webshell is simply a tiny text file (often as little as 24 bytes in size) that consists of little more than an “eval()”, which allows the attacker to execute processes on the web server. That script can be trivially obfuscated to evade signature and IOC scanning technologies.



China Chopper WebShell Controller

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

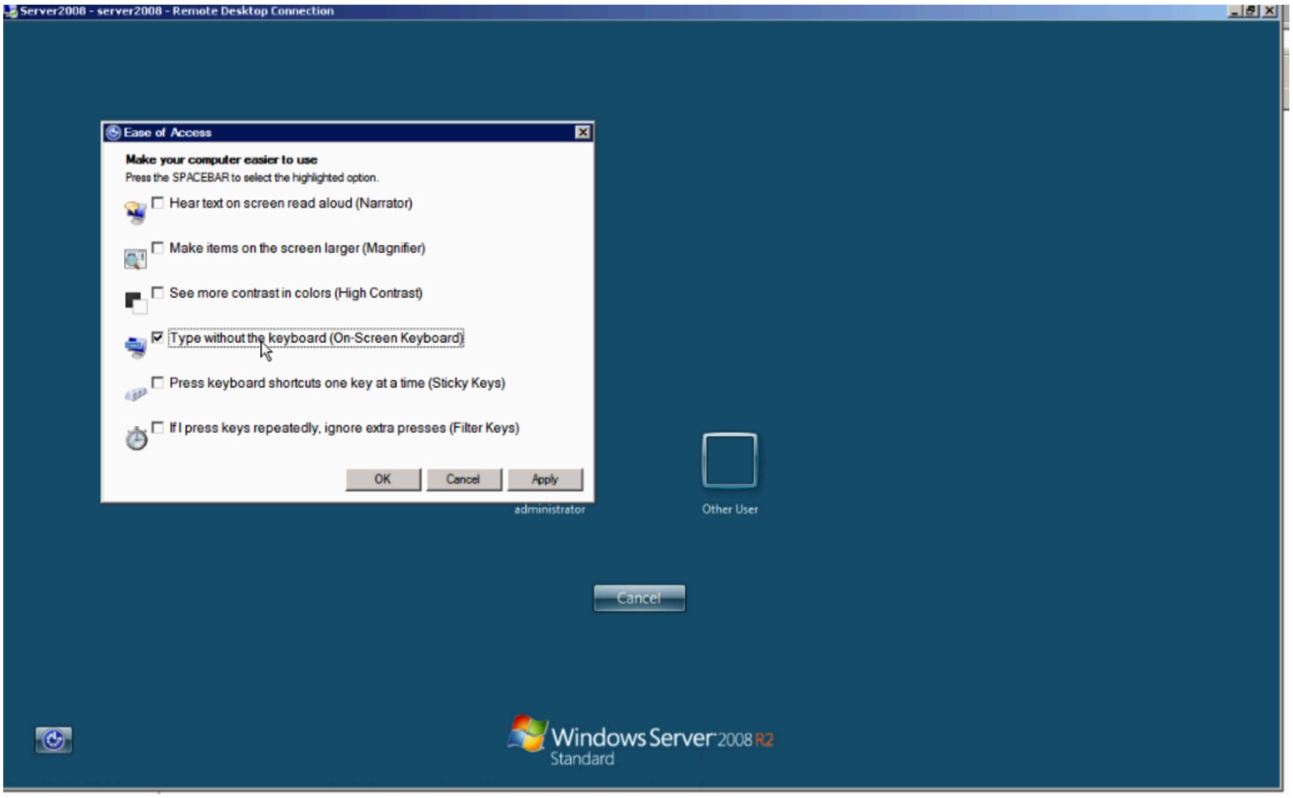
Through that webshell, the adversary then uploads a credential theft tool to steal Windows passwords and hashes, and occasionally, even Kerberos Golden Tickets that can give an adversary persistent access to the network for a decade! (Technically, one would call a tool like that malware, but usually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

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

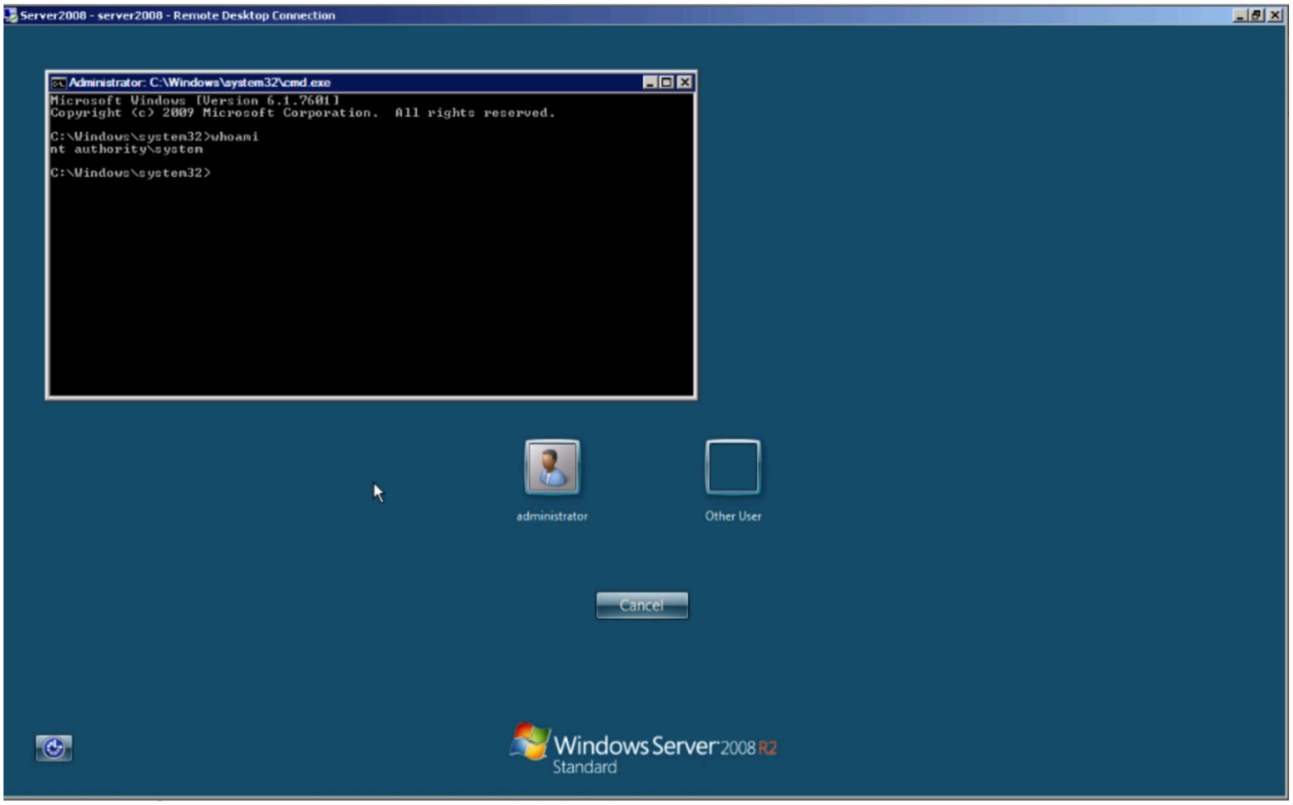
Frequently, we also see the use of the "sticky keys" trick for maintaining malware-free persistence on a victim network. With such trick, the adversary will modify the registry on a remote machine (typically using WMI) to set "cmd.exe" as a Debugger for tools like sethc.exe (Sticky Keys) and osk.exe (On-screen keyboard). Once that's done, an attacker can RDP into that machine and press the Sticky Keys or On-Screen Keyboard hotkeys and instantly get a command prompt running with System-level privileges without even requiring a login into the remote server. Thus, even if passwords are reset across the victim 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 we detected via our Falcon Host next-generation endpoint technology at a customer (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 "sticky keys" persistence trick and, afterward, copied files from remote shares via "net use," and finally used RAR to encrypt and compress the exfil data and steal it out of the network (this time, simply downloading it through the webshell).

So as you are thinking about next-generation security architecture, start thinking and asking your vendors about how they would detect such adversary tricks and the use of malware-free intrusions.

—-

And now, here's a treat for you – not only does CrowdStrike track and identify adversaries, but we also like to represent them via visual characters. Download these desktop backgrounds to remind you that the adversaries are always watching and trying to trick you into letting them inside!

Desktop Background 1:

1024 x 768 | 1280 x 1024 | 1440 x 900 | 1920 x 1200

- Putter Panda is tracked as a likely part of the 12th Bureau, 3rd GSD of the PLA (Unit 61486). It conducts significant targeting of entities in the space, aerospace, and communications sectors.

Desktop Background 2:

1024 x 768 | 1280 x 1024 | 1440 x 900 | 1920 x 1200

- A representation of some of the most popular adversaries over the past year behind our CrowdStrike “Hero”.
