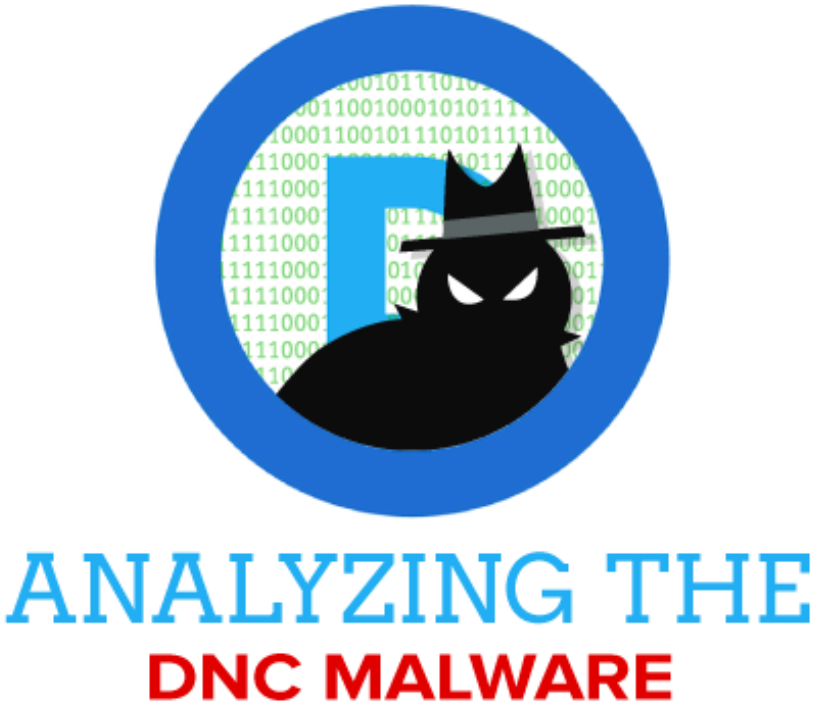
Findings from Analysis of DNC Intrusion Malware

threatgeek.com/2016/06/dnc_update.html

ThreatGeek



The Security Consulting team here at Fidelis specializes in investigations of critical security incidents by advanced threat actors. Last week, after Guccifer 2.0 claimed responsibility for the intrusion into the Democratic National Committee's (DNC) servers, we were provided with the malware samples from the CrowdStrike investigation. We performed an independent review of the malware and other data (filenames, file sizes, IP addresses) in order to validate and provide our perspective on the reporting done by CrowdStrike. This blog post provides a summary of our findings.

Many of you may be following the recent news related to the compromise of the Democratic National Committee's servers that was first reported by our colleagues over at CrowdStrike in a blog post published on June 14, 2016. Their post attributed the incident to Advanced Persistent Threat (APT) actors associated with the Russian Government named COZY BEAR and FANCY BEAR. The following day, the story got all the more interesting when an individual using the moniker Guccifer 2.0 claimed that CrowdStrike got it wrong and that he had, in fact, been the one to penetrate the DNC's servers.

We have helped hundreds of organizations deal with similar situations so we know the latest tactics, techniques, and procedures (TTPs) exceptionally well. Our analysis relies on the intelligence repository we have built through this analysis as well as Open Source Intelligence to substantiate our findings.

Before we proceed to the details of our analysis here's a quick cheat sheet on different names that security researchers have used to refer to these threat actors. However, it's important to note that actor mappings between attribution sets aren't precise. Different research methodologies and necessarily separate encounters with these actors lead to unique attribution sets. The overlaps noted here are commonly accepted.

Crowdstrike	FireEye	Palo Alto Networks	Kaspersky	Microsoft	Sample Malware Names
COZY BEAR	APT 29	CozyDuke	CozyDuke		AdobeARM, ATI-Agent, Seadaddy, Mimikatz, Seaduke and MiniDionis
FANCY BEAR	APT 28	Sofacy	Sofacy	Strontium	Sofacy, X-Agent, X-Tunnel, WinIDS, Foozer

As part of our investigation, we analyzed the same malware files that were used in the DNC incident. Here are a few highlights of our findings from reverse engineering the provided malware:

1. The malware samples matched the description, form and function that was described in the CrowdStrike blog post.

2. The malware samples contained complex coding structures and utilized obfuscation techniques that we have seen advanced adversaries utilize in other investigations we have conducted. This wasn't "Script Kiddie" stuff.

3. In addition, they were similar and at times identical to malware that other vendors have associated to these actor sets.

a. For instance, in one of their Unit 42 blog posts Palo Alto Networks provides some detailed reversing and analysis on other malware that they attributed to COZY BEAR named "SeaDuke." The Fidelis Reverse Engineering team noted that in the samples of "SeaDaddy," that were provided to us from the DNC incident, there were nearly identical code obfuscation techniques and methods. In fact, once decompiled, the two programs were very similar in form and function. They both used identical persistence methods (Powershell, a RUN registry key, and a .lnk file stored in the Startup directory).

b. The SeaDaddy sample had a self-delete function named "seppuku" which was identified in a previous SeaDuke sample described by Symantec and attributed to the COZY BEAR APT group. It's worth noting that seppuku is a Japanese word for harakiri or self-disembowelment.

c. For the X-Tunnel sample, which is malware associated with FANCY BEAR, our analysis confirmed three distinct features that are of note:

i. A sample component in the code was named "Xtunnel_Http_Method.exe" as was reported by Microsoft and attributed by them to FANCY BEAR (or "Strontium" as they named the group) in their Security Intelligence Report

Volume 19.

ii. There was a copy of OpenSSL embedded in the code and it was version 1.0.1e from February 2013 which was reported on by Netzpolitik and attributed to the same attack group in 2015.

iii. The Command and Control (C2) IPs were hardcoded into the provided sample which also matched the Netzpolotik reporting.

iv. The arguments in the sample were also identical to the Netzpolitik reporting.

4. The malware samples were conspicuously large (1.9 MB for X-Tunnel and 3.1 MB for SeaDaddy) and contained all or most of their embedded dependencies and functional code. This is a very specific modus operandi less sophisticated actors do not employ.

So what does this mean? Who is responsible for the DNC hack? Based on our comparative analysis we agree with CrowdStrike and believe that the COZY BEAR and FANCY BEAR APT groups were involved in successful intrusions at the DNC. The malware samples contain data and programing elements that are similar to malware that we have encountered in past incident response investigations and are linked to similar threat actors.

In addition to CrowdStrike, several other security firms have analyzed and published findings on malware samples that were similar and in some cases nearly identical to those used in the DNC incident. Many of these firms attributed the malware to Russian APT groups.

That brings us to the issue about Guccifer 2.0's claim of responsibility for the attack. Several researchers have raised questions about the allegedly stolen documents posted by Guccifer 2.0. Ars Technica reported similar findings that align with some of our initial analysis on this topic.

While we believe this settles the question of "who was responsible for the DNC attack," we will continue to watch, along with the rest of the security community, the new twists and turns this story takes as the U.S. presidential elections swings into full gear.

- Michael Buratowski, senior vice president, Security Consulting Services