https://www.wired.com/story/cozy-bear-dukes-russian-hackers-new-tricks/

10.17.2019 05:30 AM

Stealthy Russian Hacker Group Resurfaces With Clever New Tricks

Largely out of the spotlight since 2016, Cozy Bear hackers have been caught perpetrating a years-long campaign.

In the notorious 2016 breach of the Democratic National Committee, the group of Russian hackers known as Fancy Bear stole the show, leaking the emails and documents they had obtained in a brazen campaign to sway the results of the US presidential election. But another, far quieter band of Kremlin hackers was inside DNC networks as well. In the three years since, that second group has largely gone dark—until security researchers spotted them in the midst of another spy campaign, one that continued undetected for as long as six years.

Researchers at the Slovakian cybersecurity firm ESET today released new findings that reveal a years-long espionage campaign by a group of Kremlin-sponsored hackers that ESET refers to as the Dukes. They're also known known by the names Cozy Bear and APT29, and have been linked to Russia's Foreign Intelligence Service, or SVR. ESET found that the Dukes had penetrated the networks of at least three targets: the ministries of foreign affairs at two Eastern European countries and one European Union nation, including the network of that EU country's embassy in Washington, DC. ESET declined to reveal the identities of those victims in more detail, and note that there may well be more targets than those they've uncovered.

The researchers found that the spying campaign extend both years before the DNC hack and years after—until as recently as June of this year—and used an entirely new collection of malware tools, some of which deployed novel tricks to avoid detection. "They rebuilt their arsenal," says ESET researcher Matthieu Faou, who presented the new findings earlier this week at ESET's research conference in Bratislava, Slovakia. "They never stopped their espionage activity."

Ghost Hunters

The Dukes haven't been entirely off the radar since they were spotted inside the DNC in June of 2016. Later that year and in 2017, phishing emails believed to have been sent by to the group hit a collection of US think tanks and nongovernmental organizations, as well as the Norwegian and Dutch governments. It's not clear if any of those probes resulted in successful penetrations. Also, around a year ago, security firm FireEye attributed another widespread wave of phishing attacks to the Dukes, though ESET points out those emails delivered only publicly available malware, making any definitive link to the group tough to prove.

By contrast, the newly revealed set of intrusions—which ESET has named Ghost Hunt—managed to plant at least three new espionage tools inside target networks. It also leveraged a previously known back door, called MiniDuke, that helped ESET link the broader spy campaign with the Dukes despite

the group's recent disappearance. "They went dark and we didn’t have a lot of information," says Faou. "But over the last year and a half, we analyzed several pieces of malware, families that were initially not linked. A few months ago, we realized it was the Dukes."

In fact, one of the intrusions that included MiniDuke began in 2013, before the malware had been publicly identified—a strong indicator that the Dukes perpetrated the breach rather than someone else who picked up the malware from another source.

Trick Shots

The Dukes' new tools use clever tricks to hide themselves and their communications inside a victim's network. They include a back door called FatDuke, named for its size; the malware fills an unusual 13 megabytes, thanks to about 12MB of obfuscating code designed to help it avoid detection. To conceal its communications with a command-and-control server, FatDuke impersonates the user's browser, even mimicking the user agent for the browser that it finds on the victim's system.

The new tools also include lighter-weight implant malware ESET has named PolyglotDuke and RegDuke, each of which serves as a first-stage program capable of installing other software on a target system. Both tools have unusual means of hiding their tracks. PolyglotDuke fetches the domain of its command-and-control server from its controller's posts on Twitter, Reddit, Imgur, and other social media. And those posts can encode the domain in any of three types of written characters—hence the malware's name—Japanese katakana characters, Cherokee script, or the Kangxi radicals that serve as components of Chinese characters.

The Dukes' RegDuke implant uses a different obfuscation trick, planting a fileless back door in a target computer's memory. That back door then communicates to a Dropbox account used as its command-and-control, hiding its messages using a steganography technique that invisibly alters pixels in images like the ones shown below to embed secret information.

All of those stealth measures help to explain how the group remained undetected in these long-running intrusions for years on end, says ESET's Faou. "They were really careful, especially with network communications."

The Dukes haven't always been as successful at hiding their identity as they have been masking their intrusions. The Dutch newspaper Volksrant revealed early last year that the Dutch intelligence service AIVD compromised computers and even surveillance cameras in a Moscow-based university building the hackers were using in 2014. As a result, the Dutch spies were able to watch over the hackers' shoulders as they carried out their intrusions, and even identify everyone going into and coming out of the room where they worked. That operation led the Dutch agency to definitively identify the Dukes as agents of Russia's SVR agency, and allowed the Dutch to warn US officials of an attack in progress on the US State Department ahead of the DNC hack, alerting the US government just 24 hours after the intrusion began.

But ESET's findings show how a group like the Dukes can have a moment in the spotlight—or even under a surveillance camera—and nonetheless maintain the secrecy of some of their espionage activities for years. Just because a hacker group appears to go dark after a moment of public notoriety, in other words, doesn't mean it's not still working quietly in the shadows.

ID	Name	Description
T1566	Phishing	Later that year and in 2017, phishing emails believed to have been sent by to the group hit a collection of US think tanks and nongovernmental organizations, as well as the Norwegian and Dutch governments. Also, around a year ago, security firm FireEye attributed another widespread wave of phishing attacks to the Dukes, though ESET points out those emails delivered only publicly available malware, making any definitive link to the group tough to prove.
T1027.001	Obfuscated Files or Information: Binary Padding	They include a back door called FatDuke, named for its size; the malware fills an unusual 13 megabytes, thanks to about 12MB of obfuscating code designed to help it avoid detection.
T1071.001	Application Layer Protocol: Web Protocols	To conceal its communications with a command-and-control server, FatDuke impersonates the user's browser, even mimicking the user agent for the browser that it finds on the victim's system.
T1036.004	Masquerading: Masquerade Task or Service	To conceal its communications with a command-and-control server, FatDuke impersonates the user's browser, even mimicking the user agent for the browser that it finds on the victim's system.
T1105	Ingress Tool Transfer	The new tools also include lighter-weight implant malware ESET has named PolyglotDuke and RegDuke, each of which serves as a first-stage program capable of installing other software on a target system.
T1102	Web Service	PolyglotDuke fetches the domain of its command-and-control server from its controller's posts on Twitter, Reddit, Imgur, and other social media. And those posts can encode the domain in any of three types of written characters—hence the malware's name—Japanese katakana characters, Cherokee script, or the Kangxi radicals that serve as components of Chinese characters. The Dukes' RegDuke implant uses a different obfuscation trick, planting a fileless back door in a target computer's memory. That back door then communicates to a Dropbox account used as its command-and-control, hiding its messages using a steganography technique that invisibly alters pixels in

		images like the ones shown below to embed secret information.
T1001.002	Data Obfuscation: Steganography	The Dukes' RegDuke implant uses a different obfuscation trick, planting a fileless back door in a target computer's memory. That back door then communicates to a Dropbox account used as its command-and-control, hiding its messages using a steganography technique that invisibly alters pixels in images like the ones shown below to embed secret information.