Seedworm: Group Compromises Government Agencies, Oil & Gas, NGOs, Telecoms, and IT Firms

symantec.com/blogs/threat-intelligence/seedworm-espionage-group

Symantec researchers have uncovered extensive insights into a cyber espionage group behind a recent series of cyber attacks designed to gather intelligence on targets spread primarily across the Middle East as well as in Europe and North America.

The group, which we call Seedworm (aka MuddyWater), has been operating since at least 2017, with its most recent activity observed in December 2018.

Analysts in our DeepSight Managed Adversary and Threat Intelligence (MATI) team have found a new backdoor, Backdoor.Powemuddy, new variants of Seedworm's Powermud backdoor (aka POWERSTATS), a GitHub repository used by the group to store their scripts, as well as several post-compromise tools the group uses to exploit victims once they have established a foothold in their network.

Tracking an Attack's Footprints

In September 2018, we found evidence of Seedworm and the espionage group APT28 (aka Swallowtail, Fancy Bear), on a computer within the Brazil-based embassy of an oil-producing nation. Seeing two active groups piqued our interest and, as we began pulling on that one string, we found more clues that led us to uncover new information about Seedworm.

We not only found the initial entry point, but we were able to follow Seedworm's subsequent activity after the initial infection due to the vast telemetry Symantec has access to via its Global Intelligence Network. Because of this unique visibility, our analysts were able to trace what actions Seedworm took after they got into a network. We found new variants of the Powermud backdoor, a new backdoor (Backdoor.Powemuddy), and custom tools for stealing passwords, creating reverse shells, privilege escalation, and the use of the native Windows cabinet creation tool, makecab.exe, probably for compressing stolen data to be uploaded. DeepSight MATI customers can leverage these unique insights to combat emerging cyber threats.

Seedworm's motivations are much like many cyber espionage groups that we observe—they seek to acquire actionable information about the targeted organizations and individuals. They accomplish this with a preference for speed and agility over operational security, which ultimately led to our identification of their key operational infrastructure.

Tactics and Tools

Seedworm likely functions as a cyber espionage group to secure actionable intelligence that could benefit their sponsor's interests. During the operations, the group used tools consistent with those leveraged during past intrusions including Powermud, a custom tool used by the Seedworm group, and customized PowerShell, LaZagne, and Crackmapexec scripts.

The Seedworm group controls its Powermud backdoor from behind a proxy network to hide the ultimate command-and-control (C&C) location. The Seedworm group is the only group known to use the Powermud backdoor.

After compromising a system, typically by installing Powermud or Powemuddy, Seedworm first runs a tool that steals passwords saved in users' web browsers and email, demonstrating that access to the victim's email, social media, and chat accounts is one of their likely goals. Seedworm then uses open-source tools such as LaZagne and Crackmapexec to obtain Windows authorization credentials. Seedworm uses off-the-shelf, unmodified versions of these tools as well as custom-compiled variants which we have determined are only used by this group.

Shifting Tactics

Since its existence first came to light, we've seen Seedworm modify the way it operates. Since early 2017, they have continually updated their Powermud backdoor and other tools to avoid detection and to thwart security researchers analyzing the tools. They've also used GitHub to store malware and a handful of publicly available tools, which they then customize to carry out their work.

We have identified multiple online accounts that are likely associated with actors behind the Seedworm operations. The first finding was a public Github repository containing scripts that very closely match those observed in Seedworm operations. An additional link was then made to a persona on Twitter with similar profile data. This Twitter account follows numerous security researchers, including those who have written about the group in the past as well as developers who write the open-source tools they use.

These accounts are likely controlled by the Seedworm group. The Github repository contains a PowerShell script that has been run on victim hosts in activity attributed to Seedworm; there are also numerous Crackmapexec PowerShell commands that match victim host activity.

Choosing to rely on publicly available tools allows Seedworm to quickly update their operations by using code written by others and applying only small customizations. And they appear to adopt some of the most effective and capable tools, several of which—for these reasons—are also used by red team organizations.

Targets and Timeline

We analyzed data on 131 victims that were compromised by Seedworm’s Powermud backdoor from late September to mid-November 2018.