Sprite Spider emerging as one of the most destructive ransomware threat actors

By by Cynthia Brumfield Contributing Writer

Published: 2021-02-01 · Archived: 2026-04-05 14:33:38 UTC

Having flown under the radar for several years, the Sprite Spider group is using a ransomware code suite that is effective and hard to detect.

At the recent SANS Cyber Threat Intelligence Summit, two CrowdStrike cybersecurity leads, Senior Security Researcher Sergei Frankoff and Senior Intelligence Analyst Eric Loui, offered details on an emerging major ransomware actor they call Sprite Spider. Like many other ransomware attackers, the gang behind Sprite Spider's attacks has grown rapidly in sophistication and damage capacity since 2015. (CrowdStrike's research was echoed in a lengthy report from Palo Alto Network's Unit 42 in November 2020.)

Today Sprite Spider is poised to become one of the biggest ransomware threat actors of 2021 and has a threat profile on par with what advanced persistent threat actors were five or ten years ago. Sprite Spider's rise as a sophisticated threat is not surprising given that it, like many other organized ransomware gangs are filled with hackers who are often gainfully employed by nation-state threat actors.

Sprite Spider evolution

Sprite Spider got its start using a banking Trojan called Shifu in 2015, adding a malware loader called Vatet around 2017. In 2018, the gang deployed a remote access Trojan called PyXie. In 2019, the group evolved to the point where it deployed ransomware called DEFRAY777.

At this point, CrowdStrike researchers tied Shifu, Vatet, and PyXie to the DEFRAY777 ransomware attacks. They realized that all the activity from these components was tied to a single threat actor, which had been flying under the radar.

How the Sprite Spider ransomware works

The gang can often escape detection primarily because its code looks benign, hiding in open-source projects such as Notepad++. The only thing Sprite Spider writes to disk is Vatet, making it even harder for analysts to track them during incident response.

Despite its stealth and multiple components, Sprite Spider displays some mundane characteristics. DEFRAY777 is not sophisticated ransomware, but it gets the job done. Sprite Spider was also somewhat late to the dedicated leak site game, waiting until late November 2020 to launch its own site for communicating with victims, months after other ransomware actors began launching these sites.

The real threat from Sprite Spider escalated in July 2020 when it began targeting ESXi hosts, which are typically deployed by large organizations that use bare-metal hypervisor technology developed by VMware to manage multiple virtual machines. DEFRAY777 deployed on ESXi hosts uses stolen credentials to authenticate to vCenter, which is the web interface for managing multiple ESXi devices and websites hosted on those devices.

After that, the attackers log in, enable SSH, change SSH keys or root passwords, kill running processes and launch other tasks that lead to executing the binary in the TMP directory, encrypting all virtual machines and their hosts. Shortly after Sprite Spider began targeting ESXi hosts, another threat group called Carbon Spider also began independently targeting ESXi machines.

By targeting EXSi machines, Sprite Spider doesn't have to deploy ransomware throughout the whole organizational environment—they have to target only a few servers to encrypt a wide swath of virtualized IT infrastructure. "This is emblematic of a larger trend in the ecrime ecosystem, where some of the larger ecrime adversaries have largely shifted their operations away from banking fraud to these targeted ransomware operations," CrowdStrike's Loui said.

Commodity malware infections are precursors to ransomware attacks

Malware that was initially used as a banking Trojan has morphed into initial access tools. "Wizard Spider uses TrickBot as its initial access tool to deploy Ryuk and Conti ransomware. Indrik Spider uses Dridex for BitPaymer or WastedLocker, and Carbon Spider uses Sekur/Anunak for REvil or Darkside," Loui said. "I want to emphasize for those of you who are interfacing with CISOs or the C-suite directly, infections by so-called commodity tools or Trojans or downloaders can lead to major ransomware attacks. If you have an Emotet problem, you're probably going to have a Trickbot problem. If you have a Trickbot problem, you are going to have a Ryuk or a Conti problem."

Time is of the essence after detecting the commodity tools. "If you can't detect, respond and remediate within an hour, there's no way you're going to be able to catch up," Loui said. "So, you have to treat those potentially serious infections even if they're so-called commodity tools."

Sprite Spider kill chain comparable to nation-states ten years ago

The kill chain of Sprite Spider and some of the other emerging major ransomware groups looks a lot like the early days of how nation-state actors behaved. "It's actually almost identical to the same kill chain threat that we were dealing with ten years ago with advanced persistent threat groups," Frankoff said. "It's the same steps taken, but the objective at the end is different."

"I think we've seen a number of nation-states engage in these types of attacks to generate revenue, specifically North Korea," CrowdStrike's senior vice president of intelligence Adam Meyers tells CSO. He says that Iran and China are also getting in on the ransomware game. "It's not necessarily the nation-state that is conducting the attack, but [the cybercriminals] are using the skills they learned [by working for nation-state attackers] to make a little extra money on the side. The individuals engaged by the nation-state are conducting ransomware attacks on a moonlight shift."

Growing ransomware sophistication requires robust defenses

Whatever the case may be, ransomware attackers are growing more sophisticated and powerful all the time. “In 2020 it was clear that the sophistication and targeted use of ransomware on certain verticals was common practice by threat actors,” Mark Ostrowski, head of Engineering East for Check Point Software, tells CSO. “Clear evidence of this were attacks targeting healthcare and education networks and entities. In 2021, we can expect this to continue, and based on early reports, groups like Sprite Spider and others may specifically target interests with the biggest return.”

CrowdStrike’s Meyers has five recommendations for how organizations can best defend themselves in the face of ever-more destructive ransomware. First, “you need to prepare to defend. You have to do basic table stakes kind of stuff, things like patching,” he says.

Second, follow the one-ten-sixty rule. “You need to be able to identify things within about a minute, investigate it within about ten minutes, and respond to it in about an hour. If you can do that, you may be in a position to keep these actors from moving across your enterprise.”

Third, to cope with ransomware’s evolving nature, use next-generation protection because antivirus software does not protect against these kinds of novel threats. “Next-gen protection uses something called machine learning or artificial intelligence. Machine learning really lets you make a determination about malware or files without ever having seen it before,” Meyers says.

Fourth, practice is essential. “I always coach boards and executives to go through routine cadences of tabletop exercises.”

Finally, know who the adversaries are. “If you understand who your threat actors are, how they operate, then you’re in a better position to defend against them moving forward.”

Mark Weatherford, chief strategy officer at the National Cybersecurity Center and a former DHS cybersecurity official in the Obama administration, thinks it will take an international effort to address the growing ransomware scourge. “Until there is more of an international policy discussion, I think we’re going to see these things grow,” he tells CSO. “What we need is an international combined effort from nations around the world to say that this is no longer acceptable.” The multi-national cooperation last week that took down the Emotet infrastructure used to deliver ransomware suggests that this is now happening.
