PINCHY SPIDER Adopts “Big Game Hunting” to Distribute GandCrab

crowdstrike.com/blog/pinchy-spider-adopts-big-game-hunting/

Brendon Feeley, Bex Hartley and Sergei Frankoff March 6, 2019

CrowdStrike® Intelligence has recently observed PINCHY SPIDER affiliates deploying GandCrab ransomware in enterprise environments, using lateral movement techniques and tooling commonly associated with nation-state adversary groups and penetration testing teams. This change in tactics makes PINCHY SPIDER and its affiliates the latest eCrime adversaries to join the growing trend of targeted, low-volume/high-return ransomware deployments known as “big game hunting.”

PINCHY SPIDER is the criminal group behind the development of the ransomware most commonly known as GandCrab, which has been active since January 2018. PINCHY SPIDER sells access to use GandCrab ransomware under a partnership program with a limited number of accounts. The program is operated with a 60-40 split in profits (60 percent to the customer), as is common among eCrime actors, but PINCHY SPIDER is also willing to negotiate up to a 70-30 split for “sophisticated” customers.

GandCrab: Highly Developed and Prevalent

GandCrab has established itself as one of the most developed and prevalent ransomware families on the market. Development of the ransomware itself has been driven, in part, by PINCHY SPIDER’s interactions with the cybersecurity research community. GandCrab

contains multiple references to members of the research community who are both publicly active on social media and have reported on the ransomware.

The main catalyst for dedicated development by PINCHY SPIDER, however, has been an ongoing battle with cybersecurity providers that are actively developing GandCrab mitigations and decryptors. PINCHY SPIDER has responded by deploying fixes and even developed a zero-day exploit aimed at customers of one of those providers.

PINCHY SPIDER Advertises for Affiliates

PINCHY SPIDER has continued to promote the success of its ransomware in criminal forum posts, often boasting about public reporting of GandCrab incidents. In February, PINCHY SPIDER released version 5.2 of GandCrab, which is immune to the decryption tools developed for earlier versions of GandCrab and in fact, was deployed the day before the release of the latest decryptor.

Recently PINCHY SPIDER has also been observed advertising for individuals with remote desktop protocol (RDP) and VNC (Virtual Network Computing) skills, and spammers who have experience in corporate networking.

GandCrab Identified by CrowdStrike Intel

CrowdStrike Intelligence first identified new GandCrab ransomware deployment tactics in mid-February, when a threat actor was observed performing actions on a victim host in order to install GandCrab. Though initially unsuccessful, the threat actor returned later to perform further reconnaissance on the victim network. The following day, the threat actor returned a third time and manually removed security software from the host that was preventing the installation of GandCrab.

Using RDP and stolen credentials from the initially compromised host, the threat actor then proceeded to move laterally around the victim network and was able to deploy GandCrab across several other hosts.

Throughout the reconnaissance process, the threat actor used system administration tools such as Sysinternals Process Monitor, Process Hacker, and a file search tool called LAN Search Pro to assist with the collection of information from the hosts. Details of the affiliates, and GandCrab versions observed adopting these tactics, can be seen in Table 1.

Affiliate ID	Sub-group ID	GandCrab Version
23	23	5.2
110	1276	5.1

Table 1. GandCrab Affiiates Observed Adopting Big Game Hunting Tactics

Domain Controller Access Observed

Near the end of February, CrowdStrike Intelligence observed another incident in which similar manual lateral movement techniques were used to deploy GandCrab across multiple hosts in an enterprise. This incident began with a compromise that resulted in the threat actor gaining control of the enterprise domain controller. Once Domain Controller access was acquired, the threat actor used the enterprise's own IT systems management software, LANDesk, to deploy a loader to hosts across the enterprise.

This loader, known as Phorpiex Downloader, is not specifically tied to GandCrab or PINCHY SPIDER, and it has previously been observed dropping other malware, such as Smoke Bot, Azorult, and XMRig. In this instance, Phorpiex served two main purposes for the threat actor. First, it spread itself to all removable drives on the infected hosts in order to further propagate throughout the network. Second, it downloaded and executed GandCrab on the infected hosts.

Expanding to Adopt "Big Game Hunting" Tactics

The change in deployment tactics observed in these recent incidents, coupled with PINCHY SPIDER's advertising for individuals with skills in RDP/VNC and experience in corporate networking, suggest PINCHY SPIDER and their affiliates are expanding to adopt big game hunting tactics.

The one difference in the tactics adopted by PINCHY SPIDER, versus most other adversaries who practice big game hunting, is the monetization model. Typically, a single payment would be requested to unlock the whole enterprise, as has been observed in INDRIK SPIDER and GRIM SPIDER intrusions. However, PINCHY SPIDER is encrypting individual hosts on the enterprise network and requesting payment on a per-host basis. It should be noted that PINCHY SPIDER is not completely alone in this strategy. BOSS SPIDER used both enterprise and per-host pricing during their campaigns.

As reported in the CrowdStrike 2018 Global Threat Report, big game hunting was a trend that helped define the criminal threat landscape in 2018. This latest activity underscores the fact that additional eCrime adversaries are aspiring to adopt this operational model. Both INDRIK SPIDER (with BitPaymer ransomware) and GRIM SPIDER (with Ryuk ransomware) have made headlines with their high profile victims and ransom profits, demonstrating that big game hunting is a lucrative enterprise. Running successful big game hunting operations results in a higher average profit per victim, allowing adversaries like PINCHY SPIDER and their partners to increase their criminal revenue quickly.

Related Indicators of Compromise

IOCs
Phorpiex Loader SHA256
5a1ab27b99f3fe6cbe825f2743c77347a7339783f8a22d99a54be2d07b94c1a8

Table 2. Phorpiex IOCs Associated with Observed Activity

IOCs
GandCrab v5.1 SHA256
0741e7c0b02f6ef0b28d00a7467bf91edb0cb0f6f20dc1fbed76119c7ae79b4f

Table 3. GandCrab v5.1 IOCs Associated with Observed Activity

IOCs
GandCrab v5.2 SHA256
329b3ddbf1c00b7767f0ec39b90eb9f4f8bd98ace60e2f6b6fbfb9adf25e3ef9
bd16b703cd20e622e3e70e71bb4c68d1d1a3e14462f4b09978bbbb14e41625dc
d7ffa0d8566702474790d7cbbbf9d51e9937d82582f82e1a00ddb1c489700d62
d860bdf0d56a66f0e1b502067d07bdb595f60ef8c43de6b9caf5492a429426d6
f70d73b6c3f61f412567bf74d4f1fba052ddccf0f8b2e61a6c69de9c8c5e6ec1
fb136c8360d1a5ab80f61109c55c5a788aa1d8796d1e75aca8c1a762b598d3f4

Table 4. GandCrab v5.2 IOCs Associated with Observed Activity

Additional Resources

- *For more information on how to incorporate intelligence on dangerous threat actors into your security strategy, please visit the Falcon Threat Intelligence product page.*
- *Download the CrowdStrike 2020 Global Threat Report.*
- *Read Stories from the front lines of incident response and get insights that can help inform your security strategy in the CrowdStrike Services Cyber Intrusion Casebook.*
- *Test CrowdStrike next-gen AV for yourself. Start your free trial of Falcon Prevent™ today.*