CL0P and REvil Escalate Their Ransomware Tactics

flashpoint-intel.com/blog/cl0p-and-revil-escalate-their-ransomware-tactics/

March 11, 2021

Blogs

Blog

Over the past several weeks, Flashpoint has observed increased activity from ransomware groups REvil and CL0P. Adding new attack capabilities and more aggressive extortion techniques, the groups are rapidly extending their respective ransomware arsenals in what appears to be an escalation of both ransomware attacks and tactics.

Over the past several weeks, Flashpoint has observed increased activity from ransomware groups REvil and CL0P. Adding new attack capabilities and more aggressive extortion techniques, the groups are rapidly extending their respective ransomware arsenals in what appears to be an escalation of both ransomware attacks and tactics.

CL0P Ransomware Hones in on Accellion Breach Victims

Most recently, on March 8, 2021, CL0P began to extort the data of a new victim, Flagstar Bank, to its ransomware blog. Included in this post were samples of presumed Flagstar Bank customer and employee information—including names, partial SSNs, and physical and email addresses.

CL0P signaled that the email addresses and other personally identifiable information (PII) it posted were for sale and that they would entertain offers to purchase and obtain the data directly or pay for its deletion from the CL0P site.

Following CL0P Doxxing, Flagstar Bank Announces Unlinked Data Breach

Later on that day, Flagstar Bank issued a statement on its website detailing the likely connected and exploited vulnerability the bank uncovered due to its use of third-party vendor Accellion and its file-sharing platform; Flagstar also disclosed that some of its data had been exposed as part of this incident. The extent of Accellion's breach continues to unfold with this news, already blamed for other major breaches like Jones Day law firm.

CL0P's Multi-Pronged Extortion Ransomware to Catch On Fast

Although it's common practice for extortionist ransomware groups to exfiltrate large swaths of data prior to deploying its encryption malware, the primary objective has, historically, been to prove to ransomware victims the extent of the group's successful compromise. In these historical cases, the data is taken in a "snatch and grab" manner, without consideration given to the stolen data's value or type. Similarly, there's little to no forethought given to the selection of the sample data that the ransomware group chooses to post to its blog.

Interestingly, in this recent case with Flagstar Bank, there was no apparent or acknowledged IT environment lockdown, and thus no ransomware attack occurred by definition. However, given the sensitive and valuable nature of the Flagstar data that CL0P posted to its blog, it's clear that CL0P was at least moderately successful in its attack. By repurposing the exfiltrated data to conduct different non-ransomware extortion tactics on the same victim, CL0P extended the data's fungibility and furthered its monetization goals.

Flashpoint expects that other ransomware groups will be quick to adopt CL0P's multi-pronged extortion ransomware strategy, given the relatively minor uplift it requires to repurpose the already-stolen data.

REvil Adds DDoS and Phoning to Ransomware Arsenal

On February 25, 2021, the REvil spokesperson operating under the alias "Unknown" on the top-tier Russian-language cybercrime forums XSS and Exploit announced that the ransomware group was actively looking to add new partners to its organization to provide English-language negotiations, distributed denial-of-service (DDoS) attacks, and access to "tier 1" networks with revenue greater than $1 billion USD.

Two weeks later, on March 4, 2021, the REvil spokesperson announced another round of new capabilities, this time aimed at improving their affiliates' abilities to pressure victims into paying the ransom. These new capabilities included L3 and L7 DDoS attacks in "test mode"

and the ability to make anonymized phone calls to victims' business associates and the media.

Specifically, the REvil spokesperson announced the following on XSS [translated from Russian]:

> *"We now have the opportunity to check your networks (calls to the media, counter agents of companies) to exert maximum pressure. In order to do this, you have to indicate the domain of the company in the description of the network, who does it communicate with, and so on. You can also add contacts for spam and checking (phone numbers) to the chat."*

REvil Keeps Pace with Competitor Collectives

While these ransomware extortion tactics are new for REvil, other competitor ransomware collectives have long offered these capabilities. For instance, the ransomware groups Avaddon and Suncrypt currently use DDoS techniques as part of their ransomware TTPs. And the now-defunct Maze ransomware group and several others are known to use cold calling techniques to ratchet up extortion pressure on their victims.

Try Flashpoint's Expanded Ransomware Libraries and Response Services

With Flashpoint Ransomware Readiness and Response, we prepare enterprise customers worldwide to face ransomware attacks and actively support them as live incidents unfold.

Sign up for a risk-free 90-day trial and see Flashpoint Intelligence in action—including our recently expanded ransomware threat libraries with more data and new ways to explore and analyze targeted threats. Equipped with Flashpoint, you'll leap ahead of ransomware attacks and the cybercriminal groups who execute them.