Wipro Threat Actors Active Since 2015

BLOG MAY 1, 2019

By Jason Reaves, Joshua Platt, and Allison Nixon

As more layers of the Wipro breach are peeled away, new intelligence about the actors behind the attack on one of India's largest IT outsourcing and consulting organizations has emerged. Evidence uncovered by Flashpoint researchers links the threat actors to other malicious activity dating back to 2017, and possibly 2015, as well as the re-use of infrastructure from those older attacks.

Also, many legitimate security applications were abused during this campaign. For example, the phishing templates used to ensnare victims inside Wipro match those provided by a security awareness training provider. The attackers also dropped ScreenConnect on the machines it compromised inside Wipro, and some of the domains used in the attack were hosting powerkatz and powersploit scripts.

ScreenConnect is a remote access tool that can be used in support engagements or for remote meetings. Powerkatz is a PowerShell version of Mimikatz, a post-exploitation tool that is able to

Flashpoint Strengthens Intelligence Platform with New Dashboards and Analytics, Expanded Collections and Tailored Alerting by Industry →

meanwhile, is a collection of PowerShell modules used during penetration-testing engagements to launch exploits at a target.

Wipro has yet to publicly share any further details about the breach, which was made public April 15. According to reporting from Brian Krebs, the breach likely began earlier this year and was the precursor to further attacks against at least 11 Wipro customers. Dozens of Wipro employees were victims of phishing attacks, and the threat actors gained access to more than 100 Wipro computer systems. The ultimate aim of the group behind the Wipro attack appears to be gift-card fraud.

Inside the IOCs

Of the malicious domains and IP addresses, hashes, and file names, Flashpoint analysts were able to determine that a half-dozen were phishing domains hosting templates consistent with credential phishing attempts. The templates sought victims' Windows usernames and passwords in order to allegedly access encrypted email.

Image 1: An encrypted phishing email template

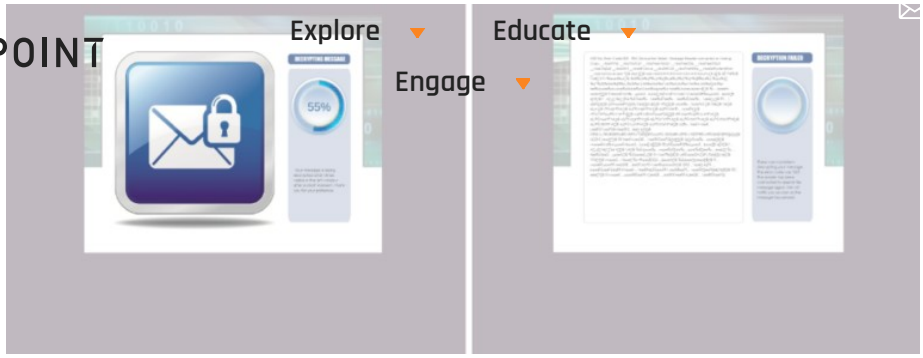


Image 2: The decrypted message templates

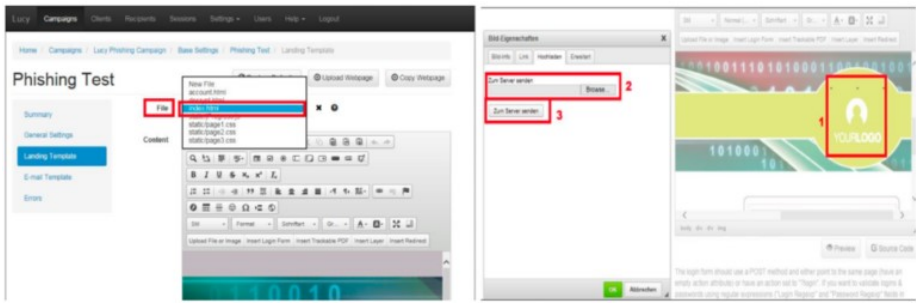


Image 3: Phishing email template configuration

The threat actors targeted the credentials of victims—in various industries—likely in order to gain access to the portals managing their gift card and rewards programs.

While investigating the phishing campaigns, analysts found evidence of attempts to spread malware called Imminent Monitor, a remote administration tool. Flashpoint was able to pivot off the file name and locate other campaigns associated with the activity, in particular a hash which led to a Word document containing a message and attachment matching the naming structure of a campaign in 2017.

The document contained a URL that redirected to a file hosted at flexmail[.]tv, which appeared to have been used multiple times to deliver documents and payloads in other campaigns. The email header, meanwhile, revealed an IP address, 123.242.230[.]14, that showed multiple malware samples communicating to it that were identified as the Netwire remote access Trojan. A number of host or campaign IDs were communicating with the IP address and all contained the same password ('!NetWire102015!') in the Netwire config.

Flashpoint Strengthens Intelligence Platform with New Dashboards and Analytics, Expanded Collections and Tailored Alerting by Industry →

Checking the sunnyvision[.]com domain that was pointed to in the email headers led to an interesting discovery, as a URL was submitted to VirusTotal linking to a ScreenConnect installer file. The header content in the VirusTotal scan shows a last-modified date of Saturday, April 13, 2019, while the URL submission appears to have occurred initially on Wednesday, April 17, 2019. It is likely the ScreenConnect installer was placed on the server on April 13, 2019. While it is possible the file is legitimately used, the file has also been identified as malicious by antivirus company McAfee.

Of the two domains not associated with phishing activity, one, xsecuremail[.]com, hosts PowerShell scripts, including 32- and 64-bit versions of powerkatz DLL files. The last modified time in the server request for the VirusTotal file is Wednesday, March 13, 2019. It is likely the file was uploaded on March 13, 2019 and possibly used in attacks around this time.

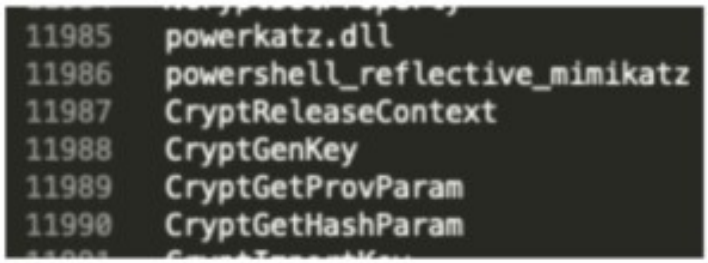


Image 5: Powerkatz DLL files

Attachments and Downloads

To download the indicators of compromise (IOCs) with the appropriate ATT&CK IDs for the Wipro incident, click here for the CSV file, and click here for the MISP.

BLOG

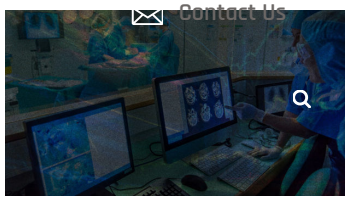
Wipro Threat Actors Active Since 2015

Evidence uncovered by Flashpoint researchers links the threat actors behind the Wipro breach to other activity dating back as early as 2015.

BLOG APRIL 30, 2019

Synthetic Identity Theft a Gateway to Business Fraud

As losses directly attributable to synthetic identity theft mount, it's inevitable that we see it leveraged for business fraud.



BLOG APRIL 22, 2019

After-Action Report: Flashpoint Remediation of 0-Day Exploit on Our Public-Facing Website

Researcher Dancho Danchev published a blog post that incorrectly reported that Flashpoint's public-facing website (flashpoint-intel.com) was "serving malware." Flashpoint's public-facing website is not and was never serving malware. We're happy to shed light on exactly what happened below.

Flashpoint Strengthens Intelligence Platform with New Dashboards and Analytics, Expanded Collections and Tailored Alerting by Industry →

Flashpoint Intelligence Brief

Subscribe to our newsletter to stay up-to-date on our latest research, news, and events

Your email address...

Subscribe →

Flashpoint Strengthens Intelligence Platform with New Dashboards and Analytics, Expanded Collections and Tailored Alerting by Industry →