PERISCOPE

July 27, 2022

TLP: AMBER

WEEKLY UNDERGROUND UPDATE

Last week in the underground, the actors **bubeL**, **Jango**, **learnrussian** and **ooo387** offered and sought to leverage point-of-sale (PoS) terminals and the actors **Beeper** and **devi0s** compromised system management providers. Additionally, the actors **Pizza**, **Rakhim** and **ShadowNatasha** offered exploits for zero-day vulnerabilities, while the actors **hinkim**, **Sonya** and the Distributed Denial of Secrets aka DDoSecrets leak website operator or operators offered data leaked from government agencies.

Threat actors offer, seek to leverage point-of-sale terminals

- On July 16, 2022, the actor **bubeL** sought to hire new members for a scam project allegedly launched by the Fight Club scam team. The actor claimed the team successfully targeted victims in China, Europe, the Middle East and the U.S. The malicious actors allegedly lure victims into making payments via phishing pages to steal payment card details and withdraw funds from victims' cards by making money transfers to accounts of merchant service providers or using PoS terminals.
- On July 17, 2022, the actor **Jango** sought fake PoS terminals to collect payment card dumps or a shimmer device designed for PoS systems. The actor was interested in any solution related to fraud involving payment processing tools.
- On July 17, 2022, the actor **learnrussian** claimed to have unauthorized access to all PoS terminals of an undisclosed Canada-based restaurant and sought someone who could upload a payment card sniffer to them. The access allegedly was gained via remote desktop protocol (RDP) and virtual network connection (VNC) account credentials.
- On July 20, 2022, the actor **ooo387** offered to sell a database collected from a PoS system used by American prepaid wireless service provider. The actor also claimed to have a database of other mobile network carriers' retail stores. The data leak allegedly includes as many as 200,000 unique employee records, most of which come with addresses, full names and email addresses or phone numbers.

Threat actors compromise system management providers

- On July 18, 2022, the actor **Beeper** sought a partner to monetize access to a managed service provider (MSP) control panel for more than 50 companies based in the U.S. with more than 100 VMware ESXi hypervisors and more than 1,000 servers. The actor claimed to be short of staff, but stated most steps of the pre-monetization phases already were complete.
- On July 19, 2022, the actor **devi0s** offered to sell unauthorized access with domain privileges to an undisclosed U.S.-based system management company. The description claimed the victim entity deals with "automation, mobile applications and management for other corporate customers with over 20 locations across North America." The actor claimed the compromised company has a revenue of more than US $500 million.

Threat actors offer exploits for zero-day vulnerabilities

- On July 15, 2022, the actor **Rakhim** offered to sell proof-of-concept (PoC) exploit code for an alleged zero-day vulnerability. The actor claimed the vulnerability allows remote code execution (RCE) and impacts Windows RDP and server message block (SMB) services.
- On July 16, 2022, the actor **ShadowNatasha** offered to sell an alleged browser-based zero-day exploit to target an email service provider. The exploit allegedly allows an attacker to bypass two-factor authentication (2FA) and reset passwords. The actor also provided a link to a PoC demonstration and offered to provide services using the exploit.
- On July 17, 2022, the actor **Pizza** offered to sell a "very expensive" exploit for a zero-day RCE vulnerability allegedly impacting a web browser. The actor claimed the vulnerability allows browser sandbox escape and is not related to the operation of the V8 JavaScript engine.

Threat actors offer data leaked from government agencies

- On July 16, 2022, the actor **Sonya** shared an archive that allegedly contains internal conversations and documents leaked from a Russian government agency. The actor claimed the leaked information demonstrates the direct influence of the state on Russian media.
- On July 19, 2022, the DDoSecrets site operator or operators released a data set allegedly exfiltrated from an Embassy in Russia. The description claimed the data leak was sourced from the Anonymous hacktivist group and contains 53.3 GB of information including 40,000 files and more than 30,000 emails from 2018 to March 2022. The same day, the operator or operators released another portion of data allegedly leaked from a government server in the U.S. The information allegedly is 2.7 GB and contains 5,000 emails dated up to Feb. 5, 2021.
- On July 20, 2022, the actor **hinkim** offered sets of documents allegedly sourced from U.S. government entities. The actor allegedly has 800 documents stored as Microsoft Word Open XML Format Document ([.]docx), Microsoft Excel ([.]xls) and portable document format ([.]pdf) files.