Published on *The National Law Review* https://natlawreview.com

Ankura CTIX FLASH Update - September 30, 2022

Article By:

Ankura Cyber Threat Investigations and Expert Services

Ransomware/Malware Activity

Royal Ransomware Operation No Longer Residing in the Shadows

"Royal", a ransomware operation consisting of "a group of vetted and experienced ransomware actors from previous operations" and first discovered in January of 2022, has quickly begun adding companies to their victim list and demanding ransoms ranging from approximately $250,000 to over $2 million. Royal was first known under the name "Zeon" but has rebranded to Royal as of mid-September 2022. Royal is known to be a private group without affiliates, unlike the common Ransomware-as-a-Service (RaaS) structure. The operation does not have a leak site, but a sample has been uploaded to a public malware repository and victims are beginning to speak out about the operation. AdvIntel CEO Vitali Kremez, in combination with Bleeping Computer, laid out details of the operation's tactics, techniques, and procedures (TTPs), as the group has been in the shadows for the majority of this year. Royal utilizes "callback phishing attacks" in which they impersonate food delivery and software providers, disguised as subscription renewal emails. From the phishing email, users are prompted to call phone numbers to "cancel the subscription" and, in turn, get socially engineered by the threat actors to install remote access software (which is utilized as initial access). This is not the only technique to gain initial access; one (1) victim has come forward stating the threat actor exploited a vulnerability in their custom web application. The Royal operation then deploys Cobalt Strike for persistence, harvests credentials, moves laterally, exfiltrates desired data, and encrypts all devices. A victim of a Royal cyberattack has also come forward stating that their virtual machines were targeted by directly encrypting the company's virtual disk files (VMDK) and that ransom notes were printed from network printers or created on the victim Windows machines. The operation's Tor negotiation site is present in the ransom note as usual and contains a simple chat functionality. Administrators should remain vigilant due to Royal having experienced actors supporting the operation and their rapid ramp-up within the last month. CTIX analysts will continue to monitor activity surrounding the Royal ransomware operation.

- Bleeping Computer: Royal Ransomware Article

Threat Actor Activity

Fancy Bear Unleashes Espionage Operation Against Defense & Government Organizations

A new operation conducted by the Fancy Bear threat organization is targeting users with malicious PowerPoint files through social engineering tactics. Fancy Bear, commonly referred to as APT28, has been active since 2004 and has been attributed to Russia's General Staff Main Intelligence Directorate military unit. These threat actors have conducted several operations including compromising the 2016 Democratic National Committee, Democratic Constitutional Campaign Committee, and presidential candidate Hilary Clinton in an attempt to interfere with United States elections. The group has also been attributed to attacks against the World Anti-Doping Agency, United States Anti-Doping Agency, Organization for the Prohibition of Chemical Weapons, and domestic nuclear facilities. In their latest espionage campaign, Fancy Bear targets defense and government organizations associated with the European Union and other Eastern European countries. Phishing emails distributed to Fancy Bear targets claim to be originating from associates of the Organization for Economic Cooperation (OECD) and include a malicious PowerPoint file that contains droppers for the Graphite malware. In short, the Graphite malware variant lives solely within computer memory and is used to deliver post-exploitation frameworks and establish communications to command-and-control (C2) servers through Microsoft OneDrive. Exfiltrated data types from this campaign have not yet been specified. CTIX analysts urges users to validate the integrity of all email communications prior to downloading any attachments or visiting embedded links to lessen the risk of threat actor compromise.

- Cysecurity: Fancy Bear Article

Vulnerabilities

New Critical Zero-day Attack-Chain Used to Exploit Vulnerable Microsoft Exchange Servers

Microsoft has announced that two (2) reported critical zero-day vulnerabilities are being actively exploited in-the-wild. The flaws are part of an attack-chain of vulnerabilities, affecting Microsoft Exchange Servers 2013, 2016, and 2019. The first vulnerability, tracked as CVE-2022-41040, is a Server-Side Request Forgery (SSRF) which allows an unauthenticated threat actor to bypass authorization, allowing them to remotely trigger the second vulnerability, which is tracked as CVE-2022-41082. This flaw is a remote code execution (RCE) vulnerability and allows the threat actors to execute arbitrary code in the target infrastructure. It should be noted that though this attack chain is quite severe, the threat actors would first have to gain initial access to the vulnerable Exchange Server. These vulnerabilities were first detected and reported to Microsoft by security researchers from the Vietnamese cybersecurity firm GTSC. The researchers determined that threat actors are exploiting the vulnerabilities to deploy “Chinese Chopper” web shells on the compromised servers. Chinese Chopper allows the threat actors to establish network persistence and exfiltrate sensitive data, as well as move latterly to infect other systems on the victims’ networks. Based on the tactics, techniques, and procedures (TTPs) of this attack, and the web shells’ code, GTSC has reasonable evidence to suspect that a Chinese threat actor is responsible. Although there are no official patches at this time, Microsoft has published manual mitigation techniques (initially provided by GTSC researchers when reporting the flaws) linked in the advisory below. CTIX analysts advise customers utilizing the affected servers to implement the mitigations and add the provided indicators of compromise for the Chinese Chopper web shell to their infrastructure. The CTIX team will continue to monitor this attack-chain and may provide an update to this piece if a Microsoft patch is made available.

- Bleeping Computer: CVE-2022-41040, CVE-2022-41082 Article

- Microsoft: CVE-2022-41040, CVE-2022-41082 Security Advisory

National Law Review, Volumess XII, Number 278