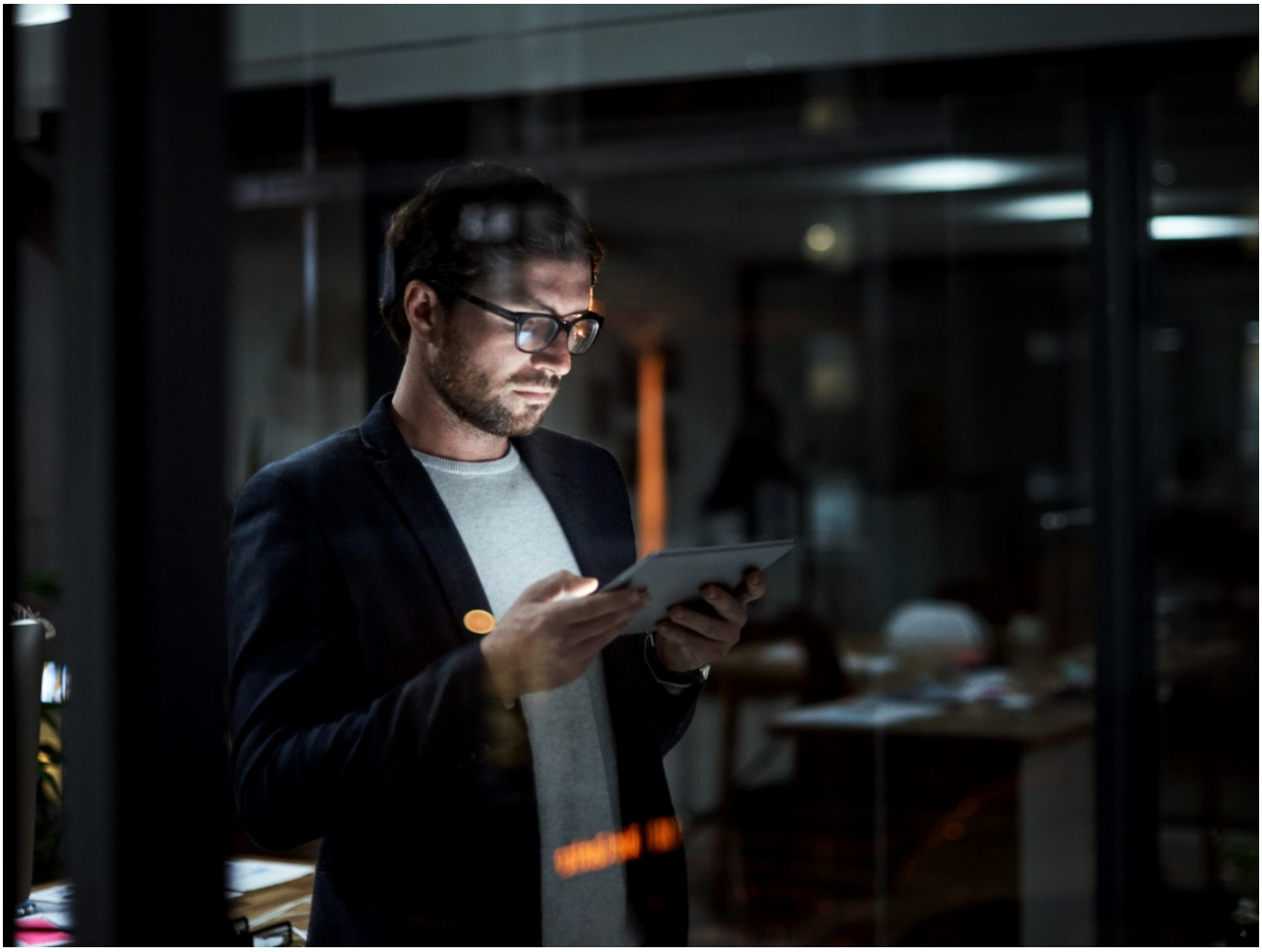
Ransomware Roundup – New Vohuk, ScareCrow, and AERST Variants

fortinet.com/blog/threat-research/ransomware-roundup-new-vohuk-scarecrow-and-aerst-variants

December 8, 2022



On a bi-weekly basis, FortiGuard Labs gathers data on ransomware variants of interest that have been gaining traction within our datasets and the OSINT community. The Ransomware Roundup report aims to provide readers with brief insights into the evolving ransomware landscape and the Fortinet solutions that protect against those variants.

This latest edition of the Ransomware Roundup covers Vohuk, ScareCrow, and AERST ransomware.

Affected platforms: Microsoft Windows
Impacted parties: Microsoft Windows Users
Impact: Encrypts files on the compromised machine and demands ransom for file decryption

Severity level: High

Vohuk Ransomware

Like most ransomware, the new Vohuk variant encrypts files on compromised machines and tries to extort money from victims. Its dropped ransom note, “README.txt”, asks victims to contact the attacker via email with a unique ID assigned to each victim. As seen in the ransom note, this Vohuk ransomware variant is version 1.3, potentially indicating that the attacker has updated the ransomware several times.

Figure 1. The Vohuk ransomware’s ransom note

Files encrypted by Vohuk ransomware have a “.Vohuk” file extension. It also replaces file icons with a red lock icon.

Figure 2. Files encrypted by Vohuk ransomware

The ransomware also replaces the desktop wallpaper with its own.

Figure 3. Desktop wallpaper replaced by Vohuk ransomware

The ransomware leaves a distinctive mutex, “Global\\VohukMutex”, which prevents different instances of Vohuk ransomware from running on the same system.

Based on the file submission locations to VirusTotal, Vohuk ransomware has primarily affected Germany and India.

ScareCrow Ransomware

ScareCrow is another typical ransomware that encrypts files on victims’ machines. Its ransom note, also titled “readme.txt”, contains three Telegram channels that victims can use to speak with the attacker. While no financial demand is requested in the ransom note, victims will most likely be asked to pay ransom to recover their encrypted files. At the time of this writing, those three Telegram channels were unavailable.

ScareCrow ransomware appears to have some similarities with the infamous Conti ransomware: both use the CHACHA algorithm to encrypt files and delete shadow copies using wmic based on shadow copy IDs. This is not all that surprising because the Conti ransomware source code was reportedly leaked earlier in the year. However, the ScareCrow threat actor put some effort into developing this ransomware variant, as our analysis found some significant differences. For example, Conti encrypts all command strings with one decryption routine, whereas ScareCrow encrypts every string, including the name of the DLLs it loads (i.e., kernel32), the name of the APIs it uses, and even the command strings with its own decryption routine.

Figure 4. ScareCrow ransomware's ransom note

ScareCrow ransomware adds a ".CROW" file extension to affected files.

Figure 5. Files encrypted by ScareCrow ransomware.

ScareCrow ransomware files were submitted to VirusTotal from Germany, India, Italy, the Philippines, Russia, and the United States. This indicates that this ransomware is relatively widespread, albeit by using unknown infection vectors.

AESRT Ransomware

AESRT is a new ransomware strain that FortiGuard Labs recently came across. It encrypts files on compromised machines and appends an ".AESRT" file extension to the files it encrypts. Instead of leaving a ransom note, the ransomware displays a popup window that includes the attacker's email address. It also accepts a field to enter the purchased key required to decrypt the ransomed files. The ransomware also deletes shadow copies, which inhibits the victim's ability to recover files.

Figure 6. Popup window displayed by AESRT ransomware

Figure 7. Files encrypted by AESRT ransomware

Fortinet Protection

Fortinet customers are already protected from these malware variants through FortiGuard's AntiVirus and FortiEDR services, as follows:

FortiGuard Labs detects known Vohuk, ScareCrow, and AESRT ransomware variants with the following AV signatures:

Vohuk ransomware

- W32/Ransom.FYWDOCB!tr.ransom
- W32/Filecoder.OKE!tr.ransom
- W32/Filecoder.RTH!tr.ransom

ScareCrow ransomware

W32/Conti.F!tr.ransom

AESRT ransomware

- MSIL/Filecoder.ACE!tr.ransom
- W32/Filecoder.ACE!tr.ransom

IOCs

Vohuk ransomware

- f570a57621db552526f7e6c092375efc8df2656c5203209b2ac8e06a198b8964
- 339a6e6e891d5bb8f19a01f948c352216e44656e46f3ee462319371fd98b3369
- 5af5401f756753bebec40c1402266d31cb16c3831cb3e9e4fe7f8562adadeee7

ScareCrow ransomware

- 7f6421cdf6355edfdcbddadd26bcdfbf984def301df3c6c03d71af8e30bb781f
- a4337294dc51518284641982a28df585ede9b5f0e3f86be3c2c6bb5ad766a50f
- bcf49782d7dc8c7010156b31d3d56193d751d0dbfa2abbe7671bcf31f2cb190a

AESRT ransomware

- 05072a7ec455fdf0977f69d49dcaaf012c403c9d39861fa2216eae19c160527f
- b6743906c49c1c7a36439a46de9aca88b6cd40f52af128b215f808a406a69598

FortiGuard Labs Guidance

Due to the ease of disruption, damage to daily operations, potential impact to an organization's reputation, and the unwanted destruction or release of personally identifiable information (PII), etc., it is vital to keep all AV and IPS signatures up to date.

Since the majority of ransomware is delivered via phishing, organizations should consider leveraging Fortinet solutions designed to train users to understand and detect phishing threats:

The FortiPhish Phishing Simulation Service uses real-world simulations to help organizations test user awareness and vigilance to phishing threats and to train and reinforce proper practices when users encounter targeted phishing attacks.

Our FREE NSE training: NSE 1 – Information Security Awareness includes a module on internet threats designed to help end users learn how to identify and protect themselves from various types of phishing attacks and can be easily added to internal training programs.

Organizations will need to make foundational changes to the frequency, location, and security of their data backups to effectively deal with the evolving and rapidly expanding risk of ransomware. When coupled with digital supply chain compromise and a workforce telecommuting into the network, there is a real risk that attacks can come from anywhere. Cloud-based security solutions, such as SASE, to protect off-network devices; advanced endpoint security, such as EDR (endpoint detection and response) solutions that can disrupt

malware mid-attack; and Zero Trust Access and network segmentation strategies that restrict access to applications and resources based on policy and context, should all be investigated to minimize risk and to reduce the impact of a successful ransomware attack.

As part of the industry's leading fully integrated Security Fabric, delivering integration and automation across your security ecosystem, Fortinet also provides an extensive portfolio of technology and human-based as-a-service offerings. These services are powered by our global FortiGuard team of seasoned cybersecurity experts.

Best Practices include Not Paying a Ransom

Organizations such as CISA, NCSC, the FBI, and HHS caution ransomware victims against paying a ransom partly because payment does not guarantee that files will be recovered. According to a U.S. Department of Treasury's Office of Foreign Assets Control (OFAC) advisory, ransom payments may also embolden adversaries to target additional organizations, encourage other criminal actors to distribute ransomware, and/or fund illicit activities that could potentially be illegal. For organizations and individuals affected by ransomware, the FBI has a Ransomware Complaint page where victims can submit samples of ransomware activity via their Internet Crimes Complaint Center (IC3).

How Fortinet Can Help

FortiGuard Labs' Emergency Incident Response Service provides rapid and effective response when an incident is detected. And our Incident Readiness Subscription Service provides tools and guidance to help you better prepare for a cyber incident through readiness assessments, IR playbook development, and IR playbook testing (tabletop exercises).

Learn more about Fortinet's FortiGuard Labs threat research and intelligence organization and the FortiGuard AI-powered security services portfolio.