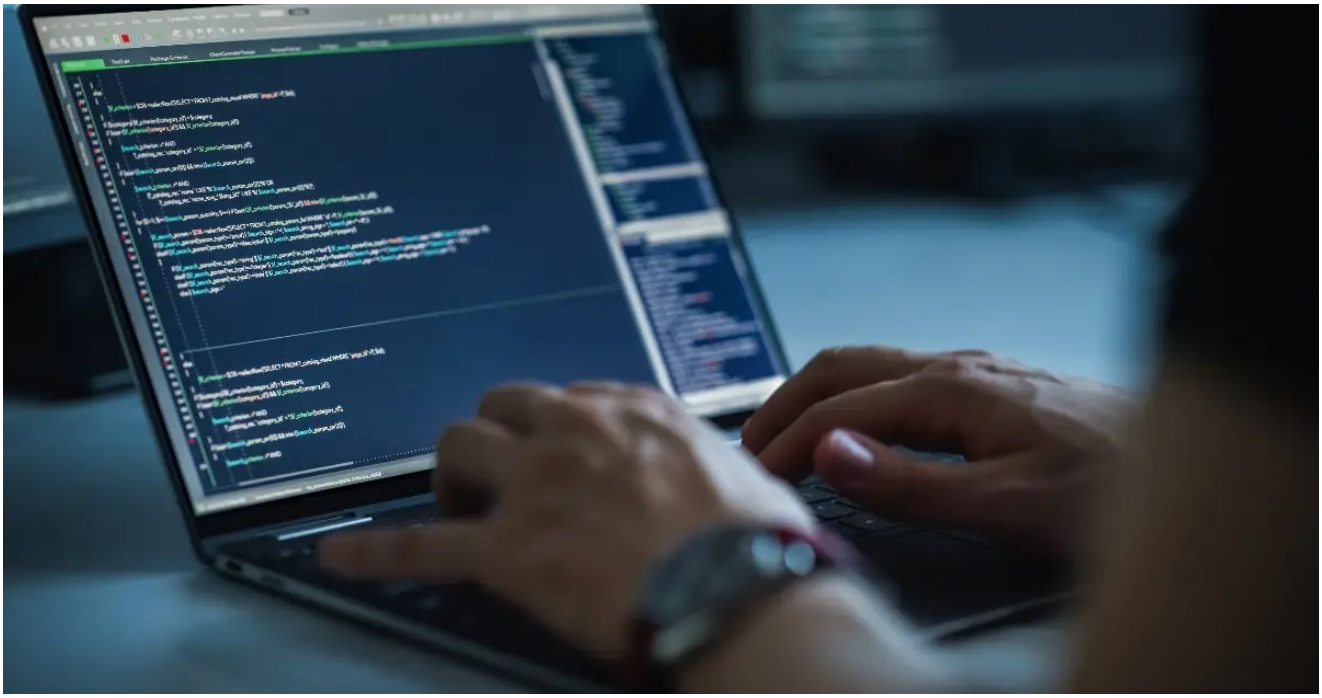
RansomExx upgrades to rust

securityintelligence.com/x-force/ransomexx-upgrades-rust/



IBM Security X-Force Threat Researchers have discovered a new variant of the RansomExx ransomware that has been rewritten in the Rust programming language, joining a growing trend of ransomware developers switching to the language.

Malware written in Rust often benefits from lower AV detection rates (compared to those written in more common languages) and this may have been the primary reason to use the language. For example, the sample analyzed in this report was not detected as malicious in the VirusTotal platform for at least 2 weeks after its initial submission. As of the time of writing, the new sample is still only detected by 14 out of the 60+ AV providers represented in the platform.

RansomExx is operated by the DefrayX threat actor group (Hive0091), which is also known for the PyXie malware, Vatet loader, and Defray ransomware strains. The newly discovered ransomware version is named RansomExx2 according to strings found within the ransomware and is designed to run on the Linux operating system. The group has historically released both Linux and Windows versions of their ransomware, so it is likely that a Windows version is also in the works.

RansomExx2 has been completely rewritten using Rust, but otherwise, its functionality is similar to its C++ predecessor. It requires a list of target directories to encrypt to be passed as command line parameters and then encrypts files using AES-256, with RSA used to protect the encryption keys.

The Rust programming language has been steadily increasing in popularity among malware developers over the course of the past year, thanks to its cross-platform support and low AV detection rates. Like the Go programming language, which has experienced a similar surge in usage by threat actors over the past few years, Rust's compilation process also results in more complex binaries that can be more time-consuming to analyse for reverse engineers.

Several ransomware developers have released Rust versions of their malware including BlackCat, Hive, and Zeon, with RansomExx2 being the most recent addition. X-Force has also analysed an ITG23 crypter written in Rust, along with the CargoBay family of backdoors and downloaders.

Analysis

The newly identified RansomExx2 sample has MD5 hash **377C6292E0852AFEB4BD22CA78000685** and is a Linux executable written in the Rust programming language.

Notable source code path strings within the binary indicate that the ransomware is a variant of RansomExx and likely named **RansomExx2**.

/mnt/z/coding/aproject/ransomexx2/ransomexx/src/parallel_iter.rs
ransomexx/src/ciphers/aes256_impl.rs
ransomexx/src/footer.rs
ransomexx/src/logic.rs
ransomexx/src/ransom_data.rs

Scroll to view full table

The website operated by the ransomware group has also been updated with the page title now listed as 'ransomexx2'.

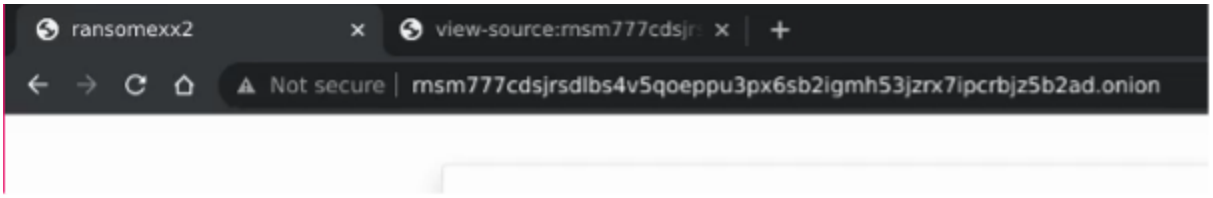


Figure 1 — A screenshot of the ransomware group's website showing the page title configured as 'ransomexx2'

Overall, the functionality of this ransomware variant is very similar to previous RansomExx Linux variants.

The ransomware expects to receive a list of directory paths to encrypt as input. If no arguments are passed to it, then it does not encrypt anything. The following command line format is required by the ransomware in order to execute correctly.

<ransomexx2_sample> –do <target_path_to_encrypt> [<additional_paths_to_encrypt> (optional)]

Scroll to view full table

Upon execution, the ransomware iterates through the specified directories, enumerating and encrypting files. All files greater than or equal to 40 bytes are encrypted, with the exception of the ransom notes and any previously encrypted files.

Each encrypted file is given a new file extension**.** It is common for RansomExx ransomware file extensions to be based on a variation of the target company name, sometimes followed by the numbers such as '911' or random characters.

A ransom note is dropped in each directory where file encryption occurs. The ransom note is named:

!_WHY_FILES_ARE_ENCRYPTED_!.txt

Scroll to view full table

The contents of this note are as follows:

Hello!

First of all it is just a business and the only thing we are interested in is money.

All your data was encrypted.

Please don’t try to modify or rename any of encrypted files, because it can result in serious data loss and decryption failure.

Here is your personal link with full information regarding this accident (use Tor browser):

http://rnsm777cdsjrsdlbs4v5qoeppu3px6sb2igmh53jzrx7ipcrbjz5b2ad.onion/<victim_id>/

Scroll to view full table

Files are encrypted using AES-256 and a randomly generated key. The AES key is itself encrypted using RSA and a hardcoded public key, and appended to the end of the encrypted file. As a result of this encryption method, the corresponding RSA private key, held by the attacker, would be required to decrypt the files.

The following RSA public key was used in the analysed sample:

```
——BEGIN PUBLIC KEY——
MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAnU8bw0DQKJjkX1QWFUM8
o52NWkUNz4zvrGRJEwhGpJZ99ho0A/BqG5kK7X9pq3GOICD3+6g928JBo6d/3cNM
Ql5lS0LaZN3bxgiNPCWFEnYjLAagRMmi8unfZmGLjc3DDKT62Q0hrI86s1zB3ZhX
6biNhXmwMaKEenpuqRBzGDqmIP9Uc9jK75SqF9T7nK1L9j+nKhYqWpeRDjDuvYPY
XHdstU0TN/OmKvPosiQaIrcIs2MNQXP7rLtMbr9knJucwLymCkF+IpMky/NTKt3u
DR+OJZZMSbmWCBATmz7P9E9Vp8jwrLzhMzEgs0G8yeseMQ2ZpZEm+MKabqkro74M
xIdocxoK2AL51ZE8c5TLYGOYbG2PAsdk/rlyRDk1diI07mCw/R4RlPcJRFDJO1eF
b1A8yp6pQjD7rg+Y38b0Z8AZzmf3aKj2B8sHOtKoNR8hKJQRtWhqKAgpQtsJY81/
2SaMLdU7yOqY34QWrGwiRei1WoJKzeyMvJjzmbTbYQYePxlbWeoV/fJ0P0IboYPH
iZ+WzXGG5Cxf7+zfZiCrbZuMqgCZdqc6ntQRcZqvw66a2Pxx4dO8AmGmxlJNzDnK
lA6CHTwDeH7BgzYDD3lJxA7ofAAzqpw8H2eyRxsqLKTI2SAnmFqk85xpxWptmhOS
BshihPaOu5a2ZXaPDeg6Lw8CAwEAAQ==
——END PUBLIC KEY——
```

Scroll to view full table

Elements such as RSA key, file extension, and the ransomware note name and contents, are encrypted within the binary and decrypted by xoring the encrypted data with an equal-sized key.

Conclusion

X-Force assesses it is highly likely that more threat actors will experiment with Rust going forward. RansomExx is yet another major ransomware family to switch to Rust in 2022 (following similar efforts with Hive and Blackcat). While these latest changes by RansomExx may not represent a significant upgrade in functionality, the switch to Rust suggests a continued focus on the development and innovation of the ransomware by the group, and continued attempts to evade detection.

To fortify your knowledge and defenses against ransomware, IBM Security has published the Definitive Guide to Ransomware 2022.

To schedule a no-cost consult with X-Force, click here.

If you are experiencing cybersecurity issues or an incident, contact X-Force to help: U.S. hotline 1-888-241-9812 | Global hotline (+001) 312-212-8034.

IBM X-Force Research | Malware | Ransomware | X-Force

Charlotte Hammond
Malware Reverse Engineer, IBM Security

POPULAR

Artificial Intelligence February 1, 2024

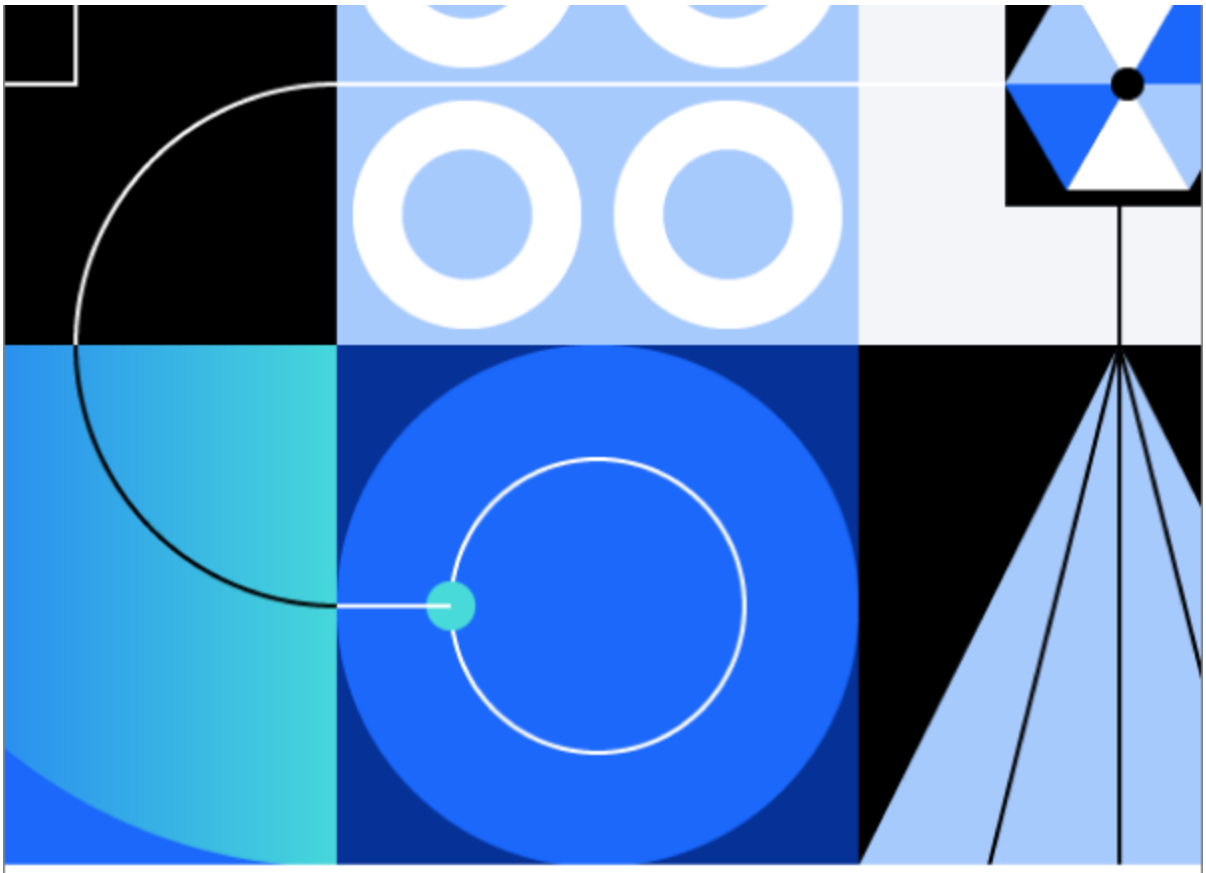
Audio-jacking: Using generative AI to distort live audio transactions

7 min read - While the evolution of LLMs mark a new era of AI, we must be mindful that new technologies come with new risks. Explore one such risk called "audio-jacking."

Risk Management January 30, 2024

Mapping attacks on generative AI to business impact

5 min read - In recent months, we've seen government and business leaders put an increased focus on securing AI models. If generative AI is the next big platform to transform the services and functions on which society as a whole depends, ensuring that…



IBM Newsletters

Get our newsletters for the latest insights on tech trends and expert thought leadership.

Subscribe today →

More from Threat Intelligence

February 1, 2024

Audio-jacking: Using generative AI to distort live audio transactions

7 min read - The rise of generative AI, including text-to-image, text-to-speech and large language models (LLMs), has significantly changed our work and personal lives. While these advancements offer many benefits, they have also presented new challenges and risks. Specifically, there has been an increase in threat actors who attempt to exploit large language models to create phishing emails and use generative AI, like fake voices, to scam people. We recently published research showcasing how adversaries could hypnotize LLMs to serve nefarious purposes simply…

December 8, 2023

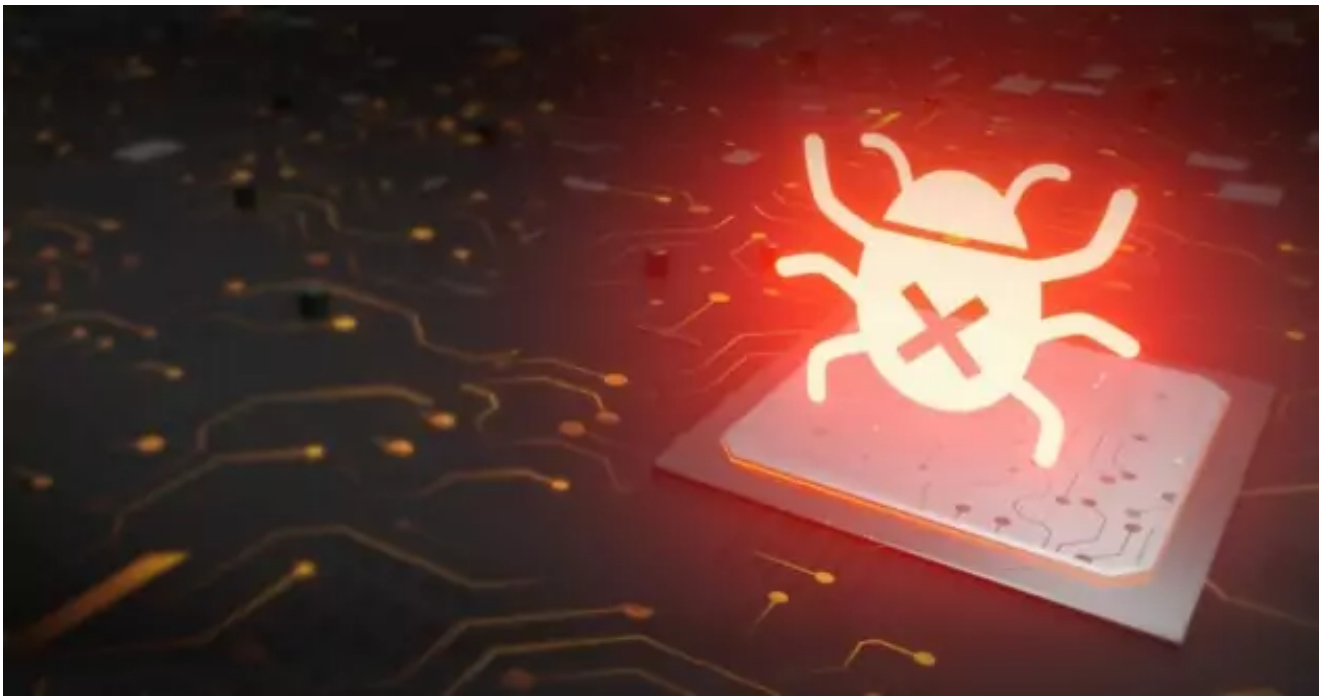
ITG05 operations leverage Israel-Hamas conflict lures to deliver Headlace malware

12 min read - As of December 2023, IBM X-Force has uncovered multiple lure documents that predominately feature the ongoing Israel-Hamas war to facilitate the delivery of the ITG05 exclusive Headlace backdoor. The newly discovered campaign is directed against targets based in at least 13 nations worldwide and leverages authentic documents created by academic, finance and diplomatic centers. ITG05's infrastructure ensures only targets from a single specific country can receive the malware, indicating the highly targeted nature of the campaign. X-Force tracks ITG05 as…

November 30, 2023

IBM identifies zero-day vulnerability in Zyxel NAS devices

12 min read - While investigating CVE-2023-27992, a vulnerability affecting Zyxel network-attached storage (NAS) devices, the IBM X-Force uncovered two new flaws, which when used together, allow for pre-authenticated remote code execution. Zyxel NAS devices are typically used by consumers as cloud storage devices for homes or small to medium-sized businesses. When used together, the flaws X-Force discovered allow a remote attacker to execute arbitrary code on the device with superuser permissions and without requiring any credentials. This results in complete control over the…



November 21, 2023

Stealthy WailingCrab Malware misuses MQTT Messaging Protocol

14 min read - This article was made possible thanks to the hard work of writer Charlotte Hammond and contributions from Ole Villadsen and Kat Metrick. IBM X-Force researchers have been tracking developments to the WailingCrab malware family, in particular, those relating to its C2 communication mechanisms, which include misusing the Internet-of-Things (IoT) messaging protocol MQTT. WailingCrab, also known as WikiLoader, is a sophisticated, multi-component malware delivered almost exclusively by an initial access broker that X-Force tracks as Hive0133, which overlaps with TA544. WailingCrab…

Topic updates

Get email updates and stay ahead of the latest threats to the security landscape, thought leadership and research.
Subscribe today

Analysis and insights from hundreds of the brightest minds in the cybersecurity industry to help you prove compliance, grow business and stop threats.