VOTIRO CLOUD

BEST IN CLASS PROTECTION AGAINST UNDISCLOSED MALWARE ATTACKS FOR THE INSURANCE SECTOR

VOTIRO

“Valyrian malware (named after the indestructible steel in the Game of Thrones) contains a range of functionality that makes it particularly devastating for anyone unfortunate enough to fall victim to it.”

400+ customers
worldwide

SONY SAMSUNG Fuji Electric MOTOROLA SIEMENS NEC NTT DATA TOKYO STOCK EXCHANGE GROUP

SETTING THE SCENE

Whilst legacy anti-virus or anti-malware solutions may be effective against known threats, they certainly do not provide adequate protection against undisclosed attacks or zero-day exploits – amongst today's most persistent and devastating attacks. For that you require a more proactive approach to threat detection and sanitization.

Here's one recent example of how Votiro Cloud's patented Content Disarm and Reconstruction (CDR) technology prevented an attack using Valyria, a particularly destructive trojan.

CUSTOMER PROFILE

Out client is a Fortune 100 insurance company. Headquartered in the US, it has offices in 29 countries across the globe. It offers a wide range of insurance products and services, including personal automobile, general liability, domestic and commercial property.

- 45,000+ employees
- Offices in over 29 countries
- Annual revenues over $40 billion +

THE ANATOMY OF AN ATTACK

Email attachments, in the form of documents, spreadsheets, PDFs and image files, are a common vehicle for malicious code. While some are easy to spot, attackers are becoming increasingly sophisticated in their hacking and phishing attempts.

In this particular instance, attackers disguised their identity by using a hacked email account, so the email appeared to be coming from a legitimate source. The email itself included a copy of the company logo in what was a convincing looking signature.

Because the email was sent from a hacked account, it bypassed the usual reputation checks carried out by the organisation's protected email gateway. Records also show that the McAfee and Sophos tools in place were up to date.

The email included a password protected ZIP file that contained a malicious word document. The unwitting recipient typed in the password to access the file, triggering the phishing attempt. This all sounds very familiar, but this is also where things change.

Instead of opening the infected word document and exposing the business to the trojan attack, the document was sanitized by Votiro and the user received a harmless document.

A PROACTIVE APROACH

For decades, we've relied on predictive analytics to detect and block malicious files. But predicting threats based on historical data is by definition imperfect. Even 99% accuracy guarantees 100% chance of attack. To be fully protected we can't just improve our predictions or threat detection. We need an entirely new approach.

Votiro Cloud leverages advanced content disarm and reconstruction (CDR) technology to proactively sanitize incoming files. Its patented solution adopts a zero-tolerance approach to file content, scanning and removing anything that shouldn't be there, returning a harmless file with 100% of the original file type functionality intact.

The key difference is that Votiro doesn't rely upon the threat being previously disclosed to provide protection. In this instance, the malware attempt was launched just 2.5 hours after it was created. The malware was first identified by traditional anti-viruses 6 days after the initial attack.

The Valyrian Trojan

Valyrian attacks are usually distributed via fake Windows updates, malicious third-party applications or weaponized attachments sent via email or social media.

Valyria is a persistent type of attack. It remains concealed within a user's system, writing itself to the Windows start-up folder via an installer. When Windows starts, programs in the start-up folder are automatically launched, meaning the malware executes and performs its malicious activities every time the computer is turned on.

VOTIRO

ABOUT VOTIRO

Established in 2010 by a team of senior cybersecurity experts, Votiro develops and licenses Votiro Cloud, a security solution based on award-winning, patented technology. With the aim of securing organisations throughout their digital transformation, Votiro is committed to allowing the safe and free use of data, with full protection against unknown threats.

Votiro CyberSec is a subsidiary of Senetas Corporation Limited (ASX:SEN)

T: +61 (0)3 9868 4555
E: infoanz@senetas.com
W: www.senetas.com