BREACH PREVENTION BLOG

CYBERSECURITY NEWS, THREAT RESEARCH, AND MORE FROM THE LEADER IN MAKING BREACH PREVENTION EASY

TRIPLE EXTORTION RANSOMWARE: A NEW CHALLENGE FOR DEFENDERS

Posted by **NUNI SNOWDEN** on September 16, 2021

Find me on: in

Tweet Share

Ransomware developers have powerful financial incentives to continue adding new features to their code. From developers to affiliates, these malicious pieces of software enrich countless cyber criminals at great expense to victims, and will likely continue to do so into the future. The average ransom demand has climbed more than 500% between 2020 and 2021, and the average payout has spiked 82% in that same period according to research from Unit 42.

Ransomware has historically focused on encryption, with the exfiltration and threatened exposure of sensitive data in a “double extortion” attack one of the most popular recent additions. However, since the financial incentives are so great, threat actors must constantly find new ways to maximize the impact of a successful attack. One of the newest ways is called “triple extortion,” which provides one more pathway to extort money from targets.

DON'T MAKE MINE A TRIPLE (RANSOMWARE THAT IS)?

Rather than the relatively simplistic efforts at turning victim downtime into profit they once were, today's ransomware attacks have become multi-layered to the point where attacks do not necessarily ever have to "end." Even the term "ransomware attack," which denotes a singular problem, is becoming a misnomer. As ransomware technologies and methods evolve, modern ransomware attack chains more closely resemble a layered hierarchy of ransomware-based threats.

Traditionally, ransomware attacks consisted of a single “stage:” a victim faced a ransom demand in return for the decryption key to unlock their systems and data. However, since 2019, when ransomware strains like DoppelPaymer evolved the capability to lock down systems and exfiltrate data simultaneously, paralyzing a victim's operations has only been the first step on the extortion ladder.

In what can be called double extortion, the threat of stolen data being published online has been a common point of leverage for criminals looking for further ransom payments. Showing how rapidly this kind of attack methodology has become the norm, more than 70 percent of ransomware attacks now also exfiltrate data.

Building on this methodology, threat actors have recently added another layer to ransomware attacks. In essence, this latest development in ransomware means that a ransomware attack doesn't just stop at the initial target. Under triple extortion, ransom demands may now also be directed at a victim's clients or suppliers. At the same time, further pressure points such as DDoS attacks, or direct leaks to the media, are also brought into the mix.

Although triple extortion was first observed barely 12 months ago, this kind of multi-layered extortion capability has rapidly become an important ransomware selling point for developers like REvil.

WHO IS VULNERABLE TO TRIPLE EXTORTION RANSOMWARE?

The most obvious targets for ransomware attacks that go beyond single or double extortion are companies and organizations that hold client or customer data as well as their own. In this respect, healthcare organizations are obvious targets.

Accordingly, the first documented example of triple extortion was seen late last year when hackers gained access to the Finnish physiotherapy provider Vastaamo. Rather than just asking for a ransom from the provider itself, threat actors also made ransom demands directly to the thousands of Vastaamo clients whose records they were able to exfiltrate.

However, any business that directly holds valuable data or can be connected to a company that does is vulnerable to triple extortion. Affiliates of REvil showcased a different version of triple extortion earlier this year when they attacked Apple after their initial victim, hardware supplier Quanta, failed to pay up. In this instance, cybercriminals used the threat that a major supplier would be compromised as leverage against their first target. For organizations in almost any sector, the reputational damage such an attack can inflict can be devastating.

AGAINST TRIPLE-LAYERED THREATS, ORGANIZATIONS ONLY HAVE ONE SHOT

While threat actors finding new ways to extort victims is essentially unsurprising, triple extortion cannot be seen as the point where the threat from ransomware stops evolving either. Instead, all it does is warn organizations that once they breach your network, threat actors will stop at nothing to get you to pay up.

What’s an organization to do in this case? Detection and response is ineffective at best against ransomware attacks, especially as many attacks wait until they reach the domain controller to deploy. By that point, detection-centric tools will have only alerted organizations to attacks they’re already in the middle of.

The best option here is to focus on prevention. Taking the steps to ensure that security holes are patched as soon as possible, educating the workforce on security awareness, and ensuring basic steps have already been taken such as applying the principles of least privilege and multi-factor authentication.

Further, with the majority of breaches starting at the endpoint, securing these is an excellent place to start. Defending your organization's endpoints against the kind of fileless ransomware delivery methods that sneak past all antivirus solutions is exactly what Morphisec Guard was built to accomplish.

Paired with Windows native security controls, Guard and the rest of the Morphisec Breach Prevention Platform hardens endpoints against attack in a way that doesn't reduce the ability of employees to get their jobs done. It's time to stop trying to react to threat actors, and time to start focusing on preventing attacks from progressing. Only then can organizations reduce the risk of any ransomware attack succeeding.

SUBSCRIBE TO OUR BLOG

Stay in the loop with industry insight, cyber security trends, and cyber attack information and company updates.

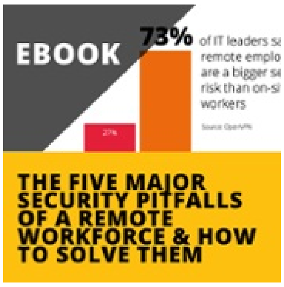
FIRST NAME*

LAST NAME*

EMAIL*

COMPANY*

SUBSCRIBE


EBOOK

73% of IT leaders sa remote emplo are a bigger se risk than on-si workers

27%

Source: OpenVPN

THE FIVE MAJOR SECURITY PITFALLS OF A REMOTE WORKFORCE & HOW TO SOLVE THEM

SEARCH OUR SITE

Keyword...

RECENT POSTS

Triple Extortion Ransomware: A New Challenge For Defenders

Move Away from “Assume Breach” to Improve Prevention

ProxyShell Exchange Exploitation Now Leads To An Increasing Amount Of Cobaltstrike Backdoors

Blocking Attacks with the Morphisec Breach Prevention Platform

Security News in Review: Are REvil and DarkSide Rebranding?

How Does MFA Fit Into a Zero Trust Endpoint Security Framework?

Is GDPR Making Ransomware Worse?

Security News in Review: Zero Trust, The Government, and You

Cyber Diplomacy: Examining the Nation-State Threat to European Businesses

Leading From Within: Netta Schmeidler, VP of Product

POSTS BY TAG

Cyber Security (98)

Endpoint Security (84)

Cyber Attacks (48)

Attack Analysis (46)

Ransomware (41)

See all