MTR in Real Time: Hand-to-hand combat with REvil ransomware chasing a $2.5 million pay day

news.sophos.com/en-us/2021/06/30/mtr-in-real-time-hand-to-hand-combat-with-revil-ransomware-chasing-a-2-5-million-pay-day/

Tilly Travers June 30, 2021

A few weeks ago, a mid-sized, 24/7 media company that had moved critical activities online during the pandemic, found itself locked in live combat with REvil ransomware attackers determined to secure a multi-million-dollar pay-out. The attack failed, but the company has yet to fully recover.

In early June 2021, a detection of Cobalt Strike on the network of a mid-size media company triggered a security alert. Cobalt Strike is a remote access agent that is widely used by adversaries as a precursor to ransomware attack.

Attackers released ransomware a few hours later at 4 am local time. For the next four hours, the target's IT team and Sophos' Rapid Response team were locked in live combat with the human adversaries orchestrating the attack.

The attack ultimately failed, but not before the attackers encrypted the data on unprotected devices, deleted online backups, and decimated one online and undefended domain.

The ransom note left on encrypted devices demanded a payment of $2.5 million and was signed by REvil, also known as Sodinokibi.

How it began

REvil is a ransomware-as-a-service offering, which means that criminal customers can lease the malware from the developers and then use their own tools and resources to target and perform the attack. The target for this particular REvil customer was a media company with approximately 600 computing devices – 25 of them servers – and three Active Directory domains, which were critical to the company's ability to maintain its 24/7 operations.

The rush to remote and online operations

Like so many organizations during the early stages of the COVID-19 pandemic, the target had rushed to equip and enable a remote workforce, and not all devices carried the same level of protection. The company also decided to internet-connect a network that was previously air-gapped. Unfortunately, these actions would come back to bite them.

Once the intruders were inside the network, they made straight for the unprotected devices and other online systems they could gain access to, installing their attack tools and using them to spread the attack to other devices.

The unfolding attack

When Sophos' Rapid Response team arrived on the scene, they discovered that the attackers had already managed to compromise a number of accounts and had been able to move unimpeded between unprotected computers.

"One of the biggest challenges for incident response is a lack of visibility about what's happening on unprotected devices," said Paul Jacobs, incident response lead, Sophos. "We can see and block inbound attacks coming from these devices to a protected endpoint, but we can't centrally remove the intruder from those devices or see what they're up to."

The team also looked at the software applications installed on devices to check for any that might be used as part of the attack.

"As a result of the pandemic, it's not unusual to find remote access applications installed on employee devices," said Jacobs. "When we saw Screen Connect on 130 endpoints, we assumed it was there intentionally to support people working from home. It turned out the company knew nothing about it – the attackers had installed the software to ensure they could maintain access to the network and compromised devices."

This was just one of several mechanisms the attackers implemented to maintain persistence. The attackers also created their own domain admin account as a fallback after stealing another set of domain admin credentials.

Hand-to-hand combat

“As the attack became noisier, the attackers knew they would be detected and blocked. We could tell that they knew we were there, and they were doing everything they could to defeat us,” said Jacobs. “Our security products have a behavioral feature called CryptoGuard that detects and blocks attempts to encrypt files even if the source is a remote, unprotected device. Once we started to see such detections, we knew the ransomware had been unleashed and the battle was on.”

The attackers tried repeatedly to breach protected devices and encrypt files, launching attacks from different unprotected devices they had been able to compromise.

Every attempt needed to be blocked and investigated to ensure there was nothing else going on and that there was no further damage – even though by then the next attack attempt was already underway. This task was made harder than normal because the organization needed to keep most of its servers online to support the 24/7 broadcasting systems.

Eventually, the onslaught began to slow down. By day two, inbound attacks were still detected intermittently but it was clear the main attack attempt was over and had failed.

The aftermath

As the incident responders and the company’s IT security team took stock, they found that damage was mainly limited to the unprotected devices and domains. The previously air-gapped, online domain was completely destroyed and needed to be rebuilt and online backups had been deleted, but the company wasn’t totally crippled by the attack, and it didn’t need to pay the exorbitant ransom. Despite this, the return to full operations has been a slow process and is ongoing at the time of publication.

The lessons learned

“In most cases, by the time we are called in the attack has already taken place, and we are there to help contain, neutralize and investigate the aftermath,” said Peter Mackenzie, manager of Sophos Rapid Response. “On this occasion we were there as the final stage of the attack unfolded and could see at first hand the determination and growing frustration of the attackers, who threw everything at us, from as many directions as they could.”

Sophos experts believe there are two important lessons defenders can take away from this incident:

1. The first is about risk management. When you make changes to your environment, for example, changing a network from air-gapped to online as in the case of this business, your level of risk changes. New areas of vulnerability open up and IT security teams need to understand and address that

2. The second is about preserving data. The first compromised account in this attack belonged to one of the IT team. All the data had been wiped and this meant that valuable information, such as details of the original breach, which could have been used for forensic analysis and investigation was lost. The more information is kept intact, the easier it is to see what happened and to ensure it can't happen again

Recommendations

Sophos recommends the following best practices to help defend against REvil and other families of ransomware and related cyber-attacks:

1. **Monitor and respond to alerts** – Ensure the appropriate tools, processes, and resources (people) are available to monitor, investigate and respond to threats seen in the environment. Ransomware attackers often time their strike during off-peak hours, at weekends or during the holidays, on the assumption that few or no staff are watching
2. **Set and enforce strong passwords** – Strong passwords serve as one of the first lines of defense. Passwords should be unique or complex and never re-used. This is easier to do if you provide staff with a password manager that can store their credentials
3. **Multi Factor Authentication (MFA)** – Even strong passwords can be compromised. Any form of multifactor authentication is better than none for securing access to critical resources such as e-mail, remote management tools, and network assets
4. **Lock down accessible services** – Perform scans of your organization's network from the outside and identify and lock down the ports commonly used by VNC, RDP, or other remote access tools. If a machine needs to be reachable using a remote management tool, put that tool behind a VPN or zero-trust network access solution that uses MFA as part of its login
5. **Segmentation and Zero-Trust** – Separate critical servers from each other and from workstations by putting them into separate VLANs as you work towards a zero-trust network model
6. **Make offline backups of information and applications**, keep them up to date and keep a copy offline
7. **Inventory your assets and accounts** – Unprotected and unpatched devices in the network increase risk and create a situation where malicious activities could pass unnoticed. It is vital to have a current inventory of all connected computers and IOT devices. Use network scans and physical checks to locate and catalog them
8. **Install layered protection** to block attackers at as many points as possible – and extend that security to all endpoints that you allow onto your network
9. **Product configuration** – Under-protected systems and devices are vulnerable too. It is important that you ensure security solutions are configured properly and to check and, where necessary, update security policies regularly. New security features are not always enabled automatically

10. **Active Directory (AD)** – Conduct regular audits on all accounts in AD, ensuring that none have more access than is needed for their purpose. Disable accounts for departing employees as soon as they leave the company
11. **Patch everything** – Keep Windows and other software up to date. This also means double checking that patches have been installed correctly and, in particular, are in place for critical systems like internet-facing machines or domain controllers

Additional advice for security leadership

1. **Understand the tactics, techniques and procedures (TTPs)** that attackers can use and how to spot the early warning signs of an imminent attack
2. **Have an incident response plan** that is continuously reviewed and updated to reflect changes in your IT environment and business operations and how they impact your security posture and level of risk
3. **Turn to external support** if you don't have the resources or expertise in house to monitor activity on the network or respond to an incident. Ransomware is often unleashed at the end of attack, so you need both dedicated anti-ransomware technology and human-led threat hunting to detect the tell-tale tactics, techniques, and procedures that indicate an attacker is in or attempting to get into the environment
4. **If you do get hit**, there are incident response experts available 24/7 you can call on to contain and neutralize the attack

Technical information on the tactics, techniques and procedures (TTPs) used in this and other REvil attacks can be found in the following companion articles, What to Expect When You've Been Hit with REvil Ransomware, and Relentless REvil, Revealed: RaaS as Variable as the Criminals Who Use It.