MTR in Real Time: Pirates pave way for Ryuk ransomware

news.sophos.com/en-us/2021/05/06/mtr-in-real-time-pirates-pave-way-for-ryuk-ransomware/

Tilly Travers May 6, 2021

Sophos' Rapid Response team was recently brought in to contain and neutralize an attack involving Ryuk ransomware. The target was a life sciences research institute that has close partnerships with local universities and works with students on various programs.

The Ryuk attack cost the institute a week's worth of vital research data, because although it had backups, they were not fully up to date. There was further operational impact when all computer and server files needed to be rebuilt from the ground up before the data could be restored. Perhaps the hardest lesson of all, however, was discovering that the attack and its impact could have been avoided with a less trusting and more robust approach to network access.

After a cyber-incident has been contained, the Rapid Response team uses the logs and historical data available to retrace the steps taken by the attackers and the tools and techniques used at every stage. In this instance, the responders found that the adversaries had gained domain access and used that to deploy the Ryuk ransomware through a series of scheduled tasks. It was only when they went all the way back to the point of initial access that they realized it led them out of the corporate network to a single human mistake and security misjudgement.

Human error can happen in any organization; the reason the mistake was able to progress to a fully-fledged attack was because the institute didn't have the protection in place to contain the error. At the heart of this was its approach to letting people outside the organization access the network. Students working with the institute use their personal computers to access the institute's network. They can connect into the network via remote Citrix sessions without the need for two factor-authentication.

The institute was exposed the moment one of these external university students apparently decided they wanted a personal copy of a data visualization software tool they were already using for work. A single user license was likely to cost them hundreds of dollars a year, so they posted a question on an online research forum asking if anyone knew of a free alternative (the Rapid Response team know this because the student handed over their laptop for analysis once the full extent of the incident became clear).

When the student couldn't find a suitable free version, they searched for a "Crack" version instead. They found what appeared to be one and tried to install it. However, the file was in fact pure malware and the installation attempt immediately triggered a security alert from Windows Defender. The user disabled Windows Defender – and at the same time appears have also disabled their firewall – and tried again. This time it worked.

However, instead of a cracked copy of the visualization tool they were after, the student got a malicious info-stealer that, once installed, began logging keystrokes, stealing browser, cookies and clipboard data and more. Somewhere along the way it apparently also found the student's access credentials for the institute's network.

Thirteen days later a remote desktop protocol (RDP) connection was registered on the institute's network using the student's credentials. It came from a computer named "Totoro," possibly after the anime character.

A feature of RDP is that a connection also triggers the automatic installation of a printer driver, enabling users to print documents remotely. This allowed the Rapid Response investigation team to see that the registered RDP connection involved a Russian language printer driver and was likely to be a rogue connection. Ten days after this connection was made the Ryuk ransomware was launched.

"It is unlikely that the operators behind the 'pirated software' malware are the same as the ones who launched the Ryuk attack," said Peter Mackenzie, manager of Rapid Response at Sophos. "The underground market for previously compromised networks offering attackers easy initial access is thriving, so we believe that the malware operators sold their access on to another attacker. The RDP connection could have been the access brokers testing their access.

“Incident investigations are crucial because they allow us to see how an attack unfolded and help targets to understand and address security gaps for the future. In this case, the implementation of robust network authentication and access controls, combined with end user education might have prevented this attack from happening. It serves as a powerful reminder of how important it is to get the security basics right.”

Recommendations

Sophos recommends taking the following actions to help defend against network access abuse:

1. Enable multi-factor authentication (MFA), where possible, for anyone required to access internal networks, including external collaborators and partners
2. Have a strong, password policy in place for everyone required to access internal networks
3. Decommission and/or upgrade any unsupported operating systems and applications
4. Review and install security software on all computers
5. Regularly review and install the latest software patches on all computers – and check they’ve been installed correctly
6. Review the use of proxy servers and regularly check security policies to prevent access to malicious websites and/or the downloading of malicious files by anyone on the network
7. Lock down remote desktop RDP access with static Local Area Network (LAN) rules, via a group policy or using access control lists
8. Implement segregation for any network access, including for LANs (or consider using virtual LANs) and where necessary use hardware/software/access control lists
9. Continuously review domain accounts and computers, removing any that are unused or not needed
10. Review firewall configurations and only whitelist traffic intended for known destinations
11. Limit the use of admin accounts by different users as this encourages credential sharing that can introduce many other security vulnerabilities

If you are facing an active threat and need immediate assistance, please contact Sophos Rapid Response for support.

Special thanks to Bill Kearney, Kyle Link, Peter Mackenzie, and Matthew Sharf, for responding to and investigating to this incident.