Nefilim Ransomware Attack Uses “Ghost” Credentials

news.sophos.com/en-us/2021/01/26/nefilim-ransomware-attack-uses-ghost-credentials/

Michael Heller January 26, 2021

Keeping close tabs on the account credentials in your organization should always be a top priority, as a Sophos Rapid Response customer recently learned. Sophos Rapid Response is a 24/7 service that helps organizations to quickly identify and neutralize active threats.

The company reached out to Rapid Response to get help with a Nefilim (also known as Nemty) ransomware attack in which more than 100 systems were impacted. Sophos’ Intercept X endpoint protection has no problem detecting and stopping Nefilim. Unfortunately, the customer did not have this protection in place. Nefilim ransomware, like virtually all major ransomware, replaces the original files with encrypted versions, making recovery impossible without either the decryption key or a recent backup.

The Rapid Response team sprang into action as soon as they were contracted by the customer, loading Sophos security onto all the systems it could access, ensuring all necessary protections were turned on for systems that already had Sophos installed, and digging for clues as to how and when the intrusion began and what might have been stolen.

By the time of Sophos’ standard “kick-off” call to describe the process of the Rapid Response team and gather context around the evidence uncovered so far, the team had already singled out user accounts that had been taken over and compiled a general timeline of the attack.

The team determined the attacker had compromised an admin account with high level access about one month before launching Nefilim ransomware. Or more accurately, the attacker gained access to that admin account, then spent one month quietly moving around to steal credentials for a domain admin account, finding the trove of data they wanted, exfiltrating hundreds of GB of data, and then finally announcing their presence with the ransomware attack.

“Ransomware is the final payload in a longer attack. It is the attacker telling you they already have control of your network and have finished the bulk of the attack. It is the attacker declaring victory,” Peter Mackenzie, manager for Rapid Response, said. “Identifying you are under a ransomware attack is easy, identifying the attacker was on your network a week earlier is what counts.”

Based on Sophos intelligence, the Rapid Response team knew the threat actors behind Nefilim ransomware commonly gain initial access either by exploiting vulnerable versions of Citrix or Remote Desktop Protocol. In this case, the adversary exploited vulnerable Citrix software, gained access to the admin account, then stole the credentials for a domain admin account using Mimikatz.

During Sophos’ initial kick-off call, the Rapid Response team relayed which admin account had been compromised in the initial intrusion, and asked the customer: Whose account was it? The answer: the account belonged to an individual who had sadly passed away around three months before the attacker’s first move.

Apparently, the account was kept active because there were services that it was used for, meaning the Rapid Response team had to discern which activities from that account were legitimate and which were malicious.

“The malicious activities were often in the middle of the night for the customer’s local time,” Mackenzie said. “We were able to work out some of the movements in the account based on when they occurred and when the commands were being performed.”

If an organization really needs an account after someone has left the company, they should implement a service account and deny interactive logins to prevent any unwanted activity. Or, if they don’t need the account for anything else, disable it and carry out regular audits of Active Directory. Active Directory Audit Policies can be set to monitor for admin account activity or if an account is added to the domain admin group.

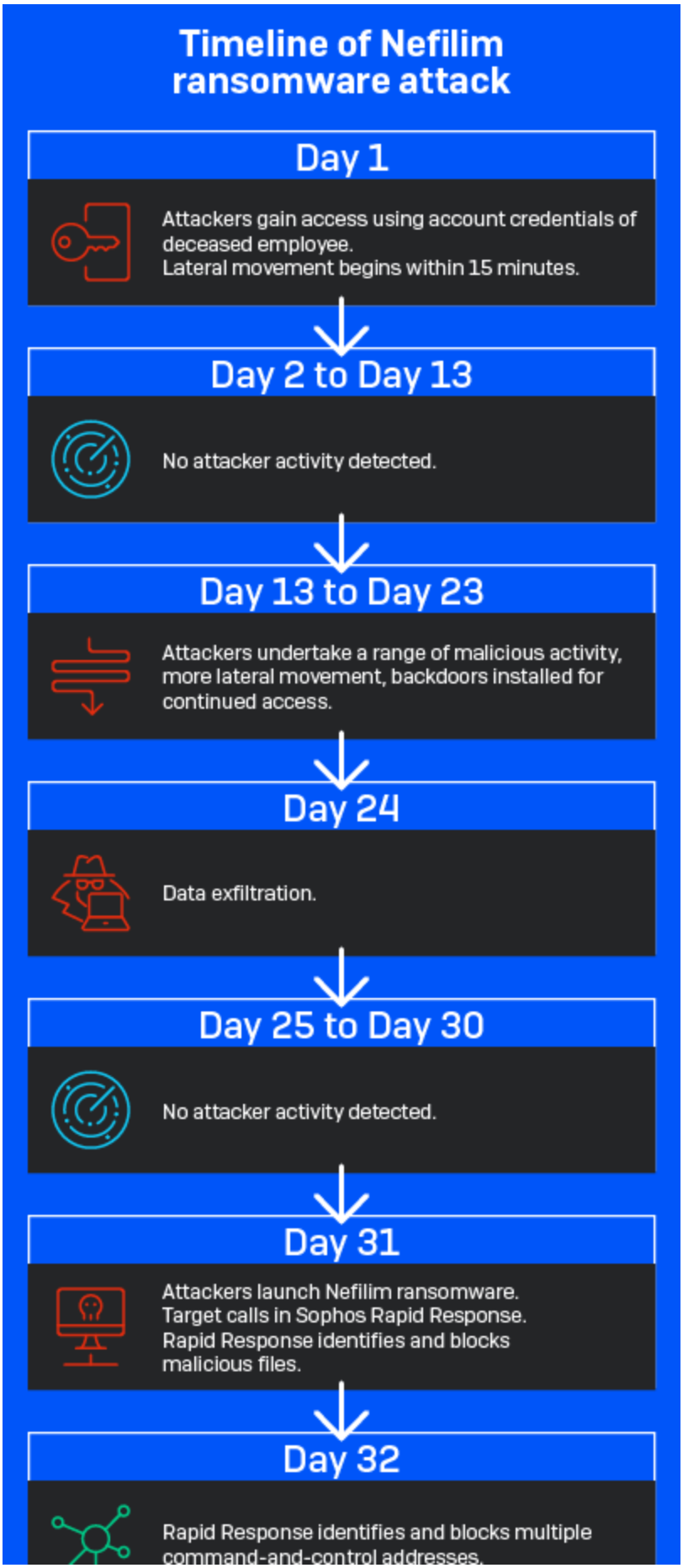
Mackenzie noted far fewer accounts need to be a domain admin than most people think.

“People assume because a person is an executive or is in charge of the network that they need to be using a domain admin account. This isn’t true and it’s dangerous,” Mackenzie said. “No account with privileges should be used by default for work that doesn’t require that level of access. Users should elevate to using the required accounts when needed and only for that task.”

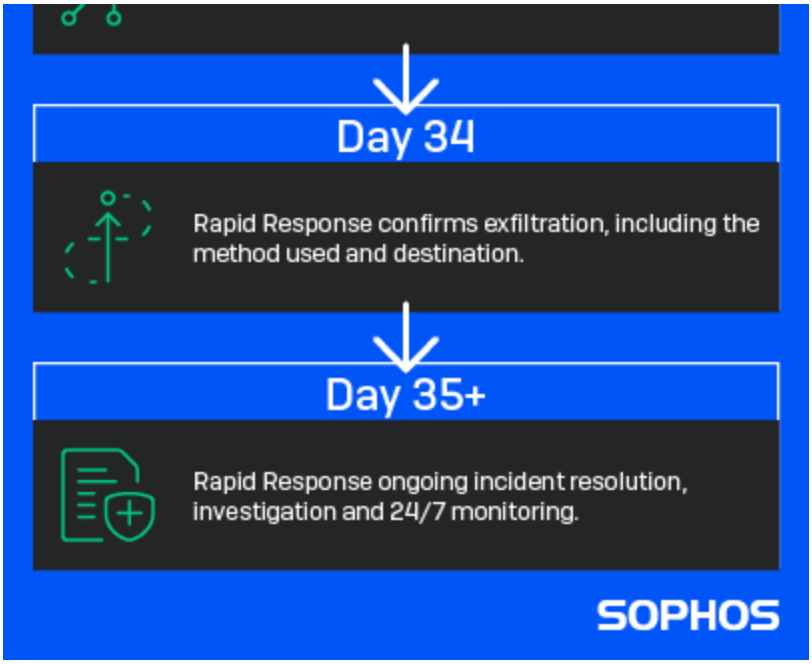
Mackenzie added that alerts should be set so that if the domain admin account is used or if a new admin account is created, someone knows. A previous case that Rapid Response was called in on proved this point.

In this particular case, an attacker gained access to an organization’s network, created a new user, and added that account to the domain admin group in Active Directory. No alerts were set off, so that new domain admin account went on to delete about 150 virtual servers and used Microsoft BitLocker to encrypt the server backups.

Mackenzie told the customer they were lucky the attack was so visibly destructive and easily noticed.



“If they hadn’t done that, how long would they have had domain admin access to the network without the customer knowing?”



Detection and IoCs

Nefilim ransomware is detected in Sophos Endpoint Protection under the definition **Troj/Ransom-GDN**.

Additional indicators of compromise have been published to the SophosLabs Github.

Nefilim group Tactics, Techniques, and Procedures (TTPs)

The common Tactics, Techniques and Procedures (TTPs) of the group(s) that operate Nefilim ransomware have often utilized Citrix vulnerabilities or Remote Desktop Protocol (RDP) to gain initial entry into victim environments by exploiting public facing applications MITRE ATT&CK T1190.

In this case, the Rapid Response team discovered vulnerable versions of Citrix software on customer systems. Although it is unclear what vulnerability was exploited, the installed Citrix Storefront 7.15 CU3 was vulnerable at time of incident to 1 Critical (CVE-2019-11634) and 4 High rated CVE vulnerabilities (CVE-2019-13608, CVE-2020-8269, CVE-2020-8270, CVE-2020-8283) which may have been exploited in order to gain initial access to the target network.

Once in, the threat actor also used Remote Desktop Protocol (RDP) logins to maintain access to the initial admin account used in the attack. On the network, the threat actor used Mimikatz, which allows the threat actors to reveal the credentials stored on the system, to compromise a domain admin account.

The Rapid Response investigation uncovered PowerShell commands as well as the use of RDP and Cobalt Strike to move laterally to multiple hosts, conduct reconnaissance, and enumerate the network.

The threat actor installed the file transfer and synchronization application MEGA in order to exfiltrate data.

The Nefilim ransomware binaries were deployed using Windows Management Instrumentation (WMI) via the compromised domain admin account.

Checklist for secure account access management

- Only grant the access permissions needed for a specific task or role
- Disable accounts no longer needed
- If you need to keep an account active after the original owner has left the organization, implement a service account and deny interactive logins
- Carry out regular audits of Active Directory: Active Directory Audit Policies can be set to monitor for admin account activity or if an unexpected account is added to the domain admin group
- Have a robust security solution in place, ideally with anti-ransomware technologies such as that featured in Intercept X

If you are experiencing an active incident and need immediate response, contact Sophos Rapid Response. For details of our 24/7 Managed Threat Response (MTR) service, visit our website or speak with your Sophos representative.

Special thanks to David Anderson, Peter Mackenzie, Sergio Bestulic, and Bill Kearney for their efforts in detecting, investigating, and responding to these threats.