MUST READ: What is a software developer? Everything you need to know about the programmer role and how it is changing

# This is how long hackers will hide in your network before deploying ransomware or being spotted

Any time is too long; but hackers are find ways to wander through networks unseen for longer than you might expect.



By Liam Tung | May 19, 2021 -- 14:07 GMT (07:07 PDT) | Topic: Security

Cyberattackers on average have 11 days after breaching a target network before they're being detected, according to UK security firm Sophos - and often when they are spotted it's because they've deployed ransomware.

As Sophos researchers note in a new report (https://news.sophos.com/en-us/2021/05/18/the-active-adversary-playbook-2021/), that's more than enough time for an attacker get a thorough overview of what a target network looks like, where its weaknesses lie, and for ransomware attackers to wreck it.

Sophos' data, based on its responses to customer incidents, suggests a much shorter "dwell time" for attackers than data from FireEye's incident response team, Mandiant, recently reported. Mandiant said the median time-to-detection was 24 days (https://www.zdnet.com/article/cybersecurity-organisations-are-getting-quicker-at-discovering-cyber-attacks-in-their-networks-but-theres-a-catch/), which was an improvement on previous years.

Sophos explains the relatively short dwell time in its incident response data is because a w[illegible] incidents it helped customers with involved ransomware — a noisy attack

that immediately triggers alarms for tech departments. So, while shorter dwell times might indicate an improvement in so-called security posture, it might also be just because file-encrypting ransomware is a disruptive attack compared to data theft.

"To put this in context, 11 days potentially provide attackers with approximately 264 hours for malicious activity, such as lateral movement, reconnaissance, credential dumping, data exfiltration, and more. Considering that some of these activities can take just minutes or a few hours to implement, 11 days provide attackers with plenty of time to do damage," notes Sophos in its Active Adversary Playbook 2021 report.

The vast majority of incidents Sophos responded to were ransomware attacks, suggesting the scale of the problem (https://www.zdnet.com/article/ransomware-just-got-very-real-and-its-likely-to-get-worse/). Other attacks include stealing data, cryptominers, banking trojans, data wipers, and the use of penetration testing tools like Cobalt Strike.

Another notable point is the widespread use by attackers of Remote Desktop Protocol (RDP) with about 30% of attacks starting with RDP and 69% of subsequent activity being conducted with RDP. Phishing, on the other hand, was the entry point for just 12% of attacks, while 10% of attacks involved exploiting an unpatched system.

Attacks on RDP endpoints have long been used to initiate ransomware attacks and are far more common than exploits against VPNs (https://www.zdnet.com/article/top-exploits-used-by-ransomware-gangs-are-vpn-bugs-but-rdp-still-reigns-supreme/). Several security firms ranked RDP as the top intrusion vector for ransomware incidents in 2020. Security firm ESET reported remote working had seen a nearly 800% spike in RDP attacks in 2020 (https://www.zdnet.com/article/big-jump-in-rdp-attacks-as-hackers-target-staff-working-from-home/).

"RDP played a part in 90% of attacks. However, the way in which attackers used RDP is worth noting. In incidents that involved RDP, it was used for external access only in just 4% of cases. Around a quarter (28%) of attacks showed attackers using RDP for both external access and internal movement, while in 41% of cases, RDP was used only for internal lateral movement within the network," Sophos threat researchers note.

Sophos also compiled a list of the most widely observed ransomware groups. DarkSide, a newish but professional ransomware service provider that started activity in mid-2020, only a % of cases Sophos investigated through 2020. It's in the spotlight because of

the attack on Colonial Pipeline (https://www.zdnet.com/article/darkside-the-ransomware-group-responsible-for-colonial-pipeline-cyberattack-explained/), which reportedly paid $5 million to the group (https://www.zdnet.com/article/colonial-pipeline-paid-close-to-5-million-in-ransomware-blackmail-payment/).

DarkSide offers its ransomware as a service to other criminal groups who distribute the ransomware, much like the REvil ransomware gang does. REvil was in the spotlight last year because of attacks on government and healthcare targets (https://www.zdnet.com/article/revil-ransomware-to-blame-for-unitingcare-queenslands-april-attack/) plus for its high ransom demands that averaged about $260,000 (https://www.zdnet.com/article/the-average-ransom-demand-for-a-revil-ransomware-infection-is-a-whopping-260000/).

According to Sophos, REvil (aka Sodinokibi) was the most active ransomware threat in 2020 along with Ryuk, which, according to some estimates, has earned $150 million through ransomware (https://www.zdnet.com/article/ryuk-ransomware-finds-foothold-in-bio-research-institute-through-a-student-who-wouldnt-pay-for-software/).

Other significant ransomware players including Dharma, Maze (defunct), Ragnarok, and Netwalker (defunct).

US president Joe Biden last week said he discussed the Colonial ransomware attack with Moscow, and suggested Russia should take "decisive action" against these attackers. The US believes DarkSide is based in Russia but not connected to the Russian government.

"We have been in direct communication with Moscow about the imperative for responsible countries to take decisive action against these ransomware networks," said Biden (https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/05/13/remarks-by-president-biden-on-the-colonial-pipeline-incident/) on May 13.

RELATED TOPICS: SECURITY TV DATA MANAGEMENT CXO DATA CENTERS



By 2021 -- 14:07 GMT (07:07 PDT) | Topic: Security