NetTraveler Malware Returns from Obscurity—What You Need to Know About the Threat

August 5, 2016
by SentinelOne

NetTraveler Returns from Obscurity—What You Need to Know About the Threat

Over 390,000 new malware variants are discovered each day, according to the independent IT security institute AV-Test. The persistent growth of the cyber threat landscape shouldn't surprise anyone at this point.

What you may not know, though, is that more than 90% of these "new" pieces of malware are actually modified versions of existing threats. In fact, even the latest zero-day attacks include elements of old attack vectors.

Staying on top of the latest threats is essential for cyber security professionals, but we can't grow complacent with dormant threats. For example, the 12-year-old NetTraveler malware toolkit has resurfaced and companies must understand how it is being used to compromise high-profile companies and address the vulnerabilities of their own organizations.

A Brief History of the NetTraveler Malware

According to Kaspersky Labs, the NetTraveler toolkit, which has been linked to a Chinese APT group, was first activated back in 2004. Despite quiet use in APT attacks after surfacing in 2004, the real NetTraveler damage came between 2010 and 2013.

In 2013, Kaspersky linked the NetTraveler malware toolkit to a cyber-espionage campaign that compromised more than 350 high-profile companies in 40 different countries. These businesses included government agencies, critical infrastructure, the oil and gas industry, military contractors and more.

The NetTraveler toolkit is generally used by APT attackers as a means of basic surveillance and data exfiltration. The malware can persist in corporate networks for long periods of time, using a keylogger to record all user activity and send the data to the attacker's command and control server.

In addition to the basic keylogs, the NetTraveler toolkit can implement a backdoor that enables attackers to steal more sensitive materials such as application configurations or design files. Even after 12 years, the Chinese APT group utilizing the NetTraveler toolkit in 2016 can still use the original functionality to compromise their Russian and Eastern European targets.

The real problem with NetTraveler today isn't the well-documented surveillance and exfiltration techniques—it's the way attackers compromise systems and deploy NetTraveler in the first place.

NetTraveler Is Deployed Through Vulnerabilities that were Patched in 2012

The NetTraveler toolkit is generally deployed via spear-phishing campaigns. The attackers attach malicious Microsoft Office documents that exploit two well-known Word vulnerabilities—CVE-2012-0158 and CVE-2010-3333. Microsoft's patch logs define these vulnerabilities as follows:

- **CVE-2012-0158**: A remote code execution vulnerability within Windows common controls. When exploited, the attacker can gain the same user rights as the logged-on user.
- **CVE-2010-3333**: This remote code execution vulnerability focuses on rich text formate (RTF) data. When exploited, attackers take complete control of the system, giving them the ability to install malicious programs, modify data, or create new user accounts.

Microsoft patched both of these vulnerabilities in 2012, but today's NetTraveler cyber-espionage campaigns are still exploiting the same vulnerabilities with malicious Office documents. The real security flaw here is that companies aren't keeping up with their patching.

Patching has generally been explained in terms of quarters—25% of companies patch within the first week, another 25% within the first month, 25% percent after one month, and 25% never patch at all. Without proper patching, attackers can fall back on dormant exploit kits like NetTraveler, catching cyber security teams off guard and compromising businesses of all sizes.

The reality is that patch mismanagement is just one way that businesses are leaving themselves vulnerable to attacks. But security software that detects exploits and malicious code using full-context behavior analysis provides a layer of coverage for unpatched systems. If you want to learn more about malware and exploit threat vectors and how to defend against them, download our free white paper, *The Wicked Truth About Malware & Exploits*.

Like this article? Follow us on LinkedIn, Twitter, YouTube or Facebook to see the content we post.

Read more about Cyber Security

- New Nation-State Threat Actor Revealed as Targeting Specific Individuals
- Breaking Down the SEO Poisoning Attack | How Attackers Are Hijacking Search Results
- Living Off Windows Defender | LockBit Ransomware Sideloads Cobalt Strike Through Microsoft Security Tool
- From the Front Lines | Hive Ransomware Deploys Novel IPfuscation Technique To Avoid Detection
- From the Front Lines | Peering into A PYSA Ransomware Attack
- Lazarus 'Operation In(ter)ception' Targets macOS Users Dreaming of Jobs in Crypto