WEBINAR SUMMARY

May 20, 2021

A Decade After Stuxnet's Printer Vulnerability: Printing is Still the Stairway to Heaven

Tomer Bar, Security Researcher and Research Team Leader, SafeBreach Labs
Peleg Hadar, Security Researcher, SafeBreach Labs
Francisco Najera, Principal Security Engineer, SafeBreach Labs

KEY TAKEAWAYS

- The propagation capabilities used by Stuxnet remain relevant to targeted attacks.
- Exploits remain in the print spooler that could lead to the next generation of Stuxnet.
- Cyberattacks are often a crime of opportunity.
- Adversarial attack automation improves an organization's security posture.

in partnership with

SafeBreach

OVERVIEW

The Stuxnet worm first appeared in 2010, initially targeting Iranian nuclear-enrichment centrifuges, but later spreading to other industrial and energy-producing facilities. Despite the significant hype around the critical Microsoft Windows Print Spooler service and a number of related patches, the attack surface remains a decade later.

Organizations can decrease the likelihood of being impacted by a next generation of Stuxnet—if it ever comes to be—or by any attack, by using attack automation. Solutions like the SafeBreach platform give security teams the tools they need to run actual real-world attacks in a controlled manner, allowing them to identify and close gaps before a real attack occurs.

CONTEXT

Peleg Hadar and Tomer Bar discussed Stuxnet and shared some of the related vulnerabilities they and other researchers have discovered since the worm was first seen in 2010. Francisco Najera discussed how adversarial attack automation can help organizations protect against cyberattacks.

KEY TAKEAWAYS

The propagation capabilities used by Stuxnet remain relevant to targeted attacks.

The Stuxnet worm can be broken down into three parts:

1. Propagation to the target network
2. Evasion techniques that allow the worm to operate under the radar
3. An industrial control systems (ICS) payload

Although Microsoft patched the initial propagation vulnerabilities in 2010, related security holes remain relevant to targeted attacks.

Figure 1: The main building blocks of Stuxnet: propagation, evasion, and ICS

> A decade after Stuxnet, the most interesting part is definitely the propagation capabilities, which are still relevant in almost any targeted attack.
>
> *Tomer Bar*

Stuxnet exploited propagation vulnerabilities in four areas: link (LNK) shortcut files, remote procedure calls (RPCs), Task Scheduler, and Win32k. Although these were patched by Microsoft, additional common vulnerabilities and exposures (CVEs) have been identified, some of which have also been patched.

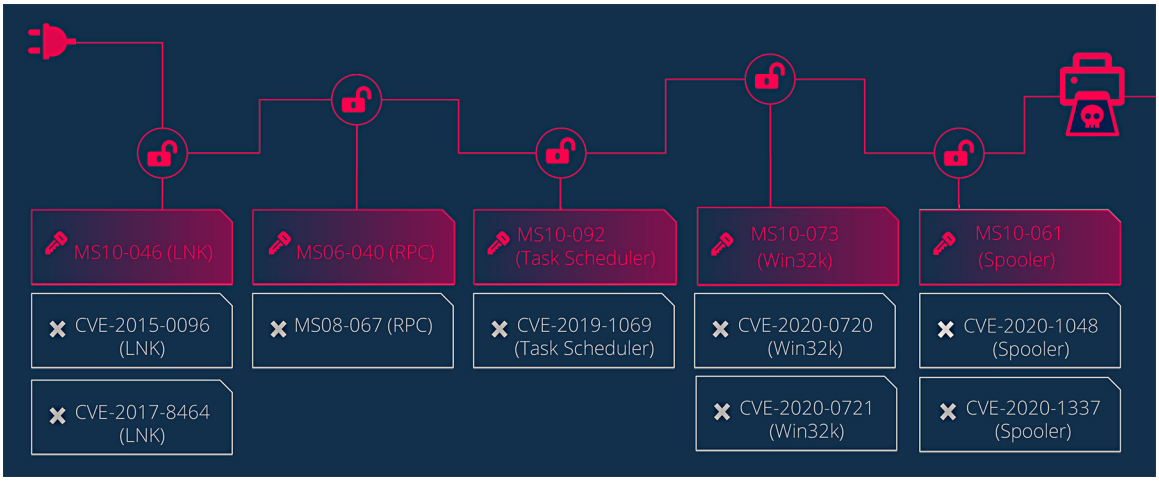
Table 1: Propagation vulnerabilities exploited by Stuxnet led to related security holes

Exploitation Path	How it was used
LNK	Weaponized universal serial bus (USB) flash drives traveled between internet-facing and internal network computers to execute a malicious dynamic link library (DLL) file. In addition to the initial 2010 problem, additional vulnerabilities were found and patched in 2015 and 2017.
RPC	A limited scope vulnerability was found in 2006; in 2009, the same DLL was widely exploited by Stuxnet and the Conficker worm. The vulnerability caused a stack-based buffer overflow, allowing attackers to gain control over the input buffer pointer, which enabled out-of-path writing. These vulnerabilities were patched by Microsoft.
Task Scheduler	Stuxnet exploited a collision-prone algorithm to forge extensible markup language (XML) files. These forged files executed jobs that enabled local privilege escalation (LPE) on the system. A second Task Scheduler LPE was found and patched in 2019.
Win32k	Numerous Win32k vulnerabilities allowed Stuxnet to escalate privileges. As of 2020, many Win32k LPE vulnerabilities remain.

Exploits remain in the print spooler that could lead to the next generation of Stuxnet.

The spooler printing exploits identified by the SafeBreach Labs team and other security researchers, like CrowdStrike, could lead to a "Stuxnet 2.0" or something similar. These teams are reporting these vulnerabilities, but some remain.

Figure 2: Current spooler printing vulnerabilities open the path for exploits



> Now that we have cobbled the [exploits] together, we have found equivalent capabilities to potentially build the Stuxnet 2.0 propagation part.
>
> *Peleg Hadar*

Keeping endpoints updated with the latest patches can help with system security, but because vulnerabilities remain, it may not be enough. One problem is that with LPE, a limited user can write directly to several locations later being used by a privileged service. The SafeBreach team has created a generic proof of concept mini field driver and associated print spooler research tools that anyone can use to restrict file write operations by a limited user.

Cyberattacks are often a crime of opportunity.

Some cyberattacks are complex, and the attackers behind them are highly motivated and sophisticated. Many attacks are opportunistic, taking advantage of system misconfigurations or a workforce that quickly shifted to remote due to the pandemic.

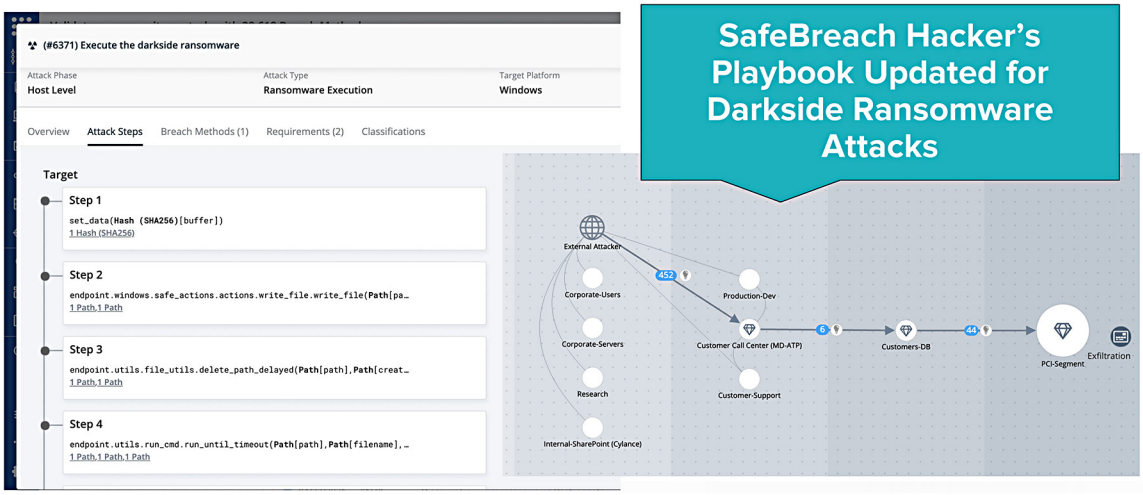
> Not all attacks are sophisticated. A lot of these attacks are simply a crime of opportunity.
>
> *Francisco Najera*

Businesses often struggle with defending against attacks. Not only do they lack the complete system visibility that enables them to identify potential security holes, but they don't have enough people available to ensure their systems are secure. Analyst burnout and organizational churn also contribute, leaving companies exposed and lacking institutional knowledge about their environment, ultimately exposing more cracks that adversaries can jump on and establish a foothold.

Adversarial attack automation improves an organization's security posture.

Organizations can use adversarial attack automation to help them identify and address gaps in their security. Attack automation, like that available from SafeBreach, provides security teams with everything they need to launch attacks against their own systems using real-world threats, allowing them to validate the efficacy of the security controls in their environment.

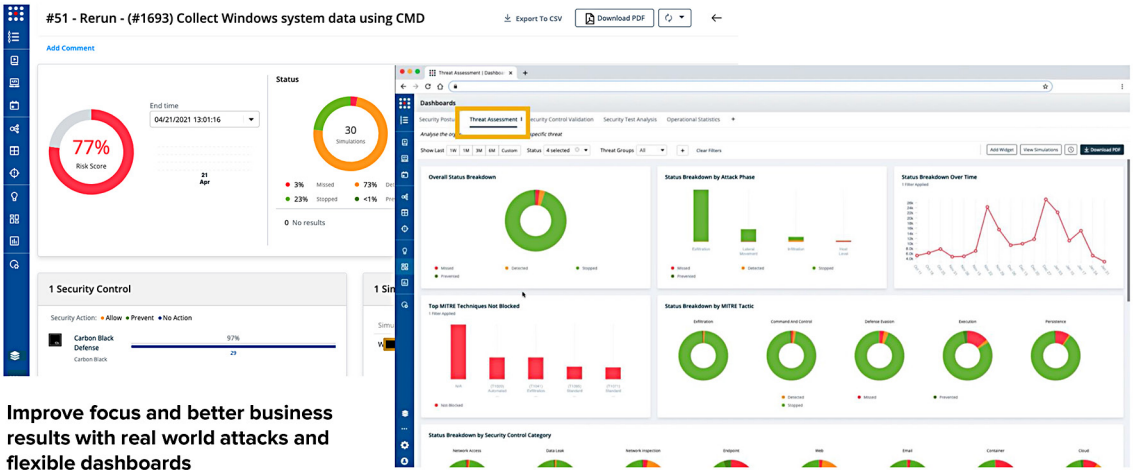
Figure 3: SafeBreach allows organizations to automate real-world attacks to test security



The SafeBreach platform includes more than just the tools to provide basic attack coverage for common tactics, techniques, and procedures (TTPs). The platform includes:

- **A hacker's playbook** that is frequently updated with the latest information on attacks, alerts, TTPs, and indicators of compromise (IOCs), as well as content to easily launch fully automated attack campaigns to validate controls.
- **Bring your own attacks,** which allows organizations to easily create and run their own attacks to validate specific scenarios within their environment.
- **Flexible dashboards** that improve visibility into the gaps and issues identified during the automated attack, so that those problems can be resolved quickly.

Figure 4: SafeBreach's flexible dashboards support visibility into identified security gaps



BIOGRAPHIES

Tomer Bar

Security Researcher and Research Team leader, SafeBreach Labs

Tomer Bar is a security researcher and a research team leader with 15+ years of unique experience in the sec field. Currently, he leads the SafeBreach Labs research team. His experience involved vulnerability research and malware analysis. He is a recognized industry speaker, having spoken at DEF CON, Black Hat USA.

Peleg Hadar

Security Researcher, SafeBreach Lab

Peleg Hadar (@peleghd) is a security researcher, having 8+ years of unique experience in the sec field. Currently, he is doing research @SafeBreach Lab after serving in various sec positions @IDF. His experience involved security from many angles: starting with network research, and now mostly software research. Peleg likes to investigate mostly Microsoft Windows components. He presented his research at Black Hat USA and DEF CON.

Francisco Najera, CISSP, CISM

Principal Security Engineer, SafeBreach Labs

Francisco Najera is an information security professional with over 20 years of experience. Over the last two decades, he has held multiple roles ranging from security architect and solutions engineer to technical lead and global director, advising and developing successful solutions for a diverse group of enterprises. At SafeBreach, he is focused on evangelizing the value of adversary simulation and helping clients measure the effectiveness of their security controls in order to drive continuous improvement of their security programs.