Tech Talk

ONE CLICK FIX

Mar. 2024 | Issue No. 15

What is LOTL?

Ransomware gangs often operate under the ethos of "If it ain't broke, break it—but keep it quiet," a stark contrast to the familiar saying "If it ain't broke, don't fix it." In recent times, the threat landscape for organizations, regardless of size, has been significantly impacted by the rise of cyberattacks, notably fueled by the proliferation of Ransomware-as-a-Service (RaaS) groups.

Between July 2022 and June 2023, a total of 1,900 ransomware incidents were reported across the US, Germany, France, and the UK alone, highlighting the severity of the situation. Noteworthy tactics employed by ransomware actors include supply chain infiltrations, double and triple extortion schemes, and exploiting system vulnerabilities.

However, one particularly insidious method gaining prevalence is known as Living Off The Land (LOTL). LOTL attacks involve cybercriminals utilizing legitimate IT tools like PowerShell, PS Exec, or Windows Management Instrumentation to carry out malicious activities. These attacks fall under the category of advanced persistent threats, leveraging existing system components such as binaries, scripts, administrative functions, drivers, and batch files to execute commands, alter system settings, exfiltrate sensitive data, and establish control over the targeted network.

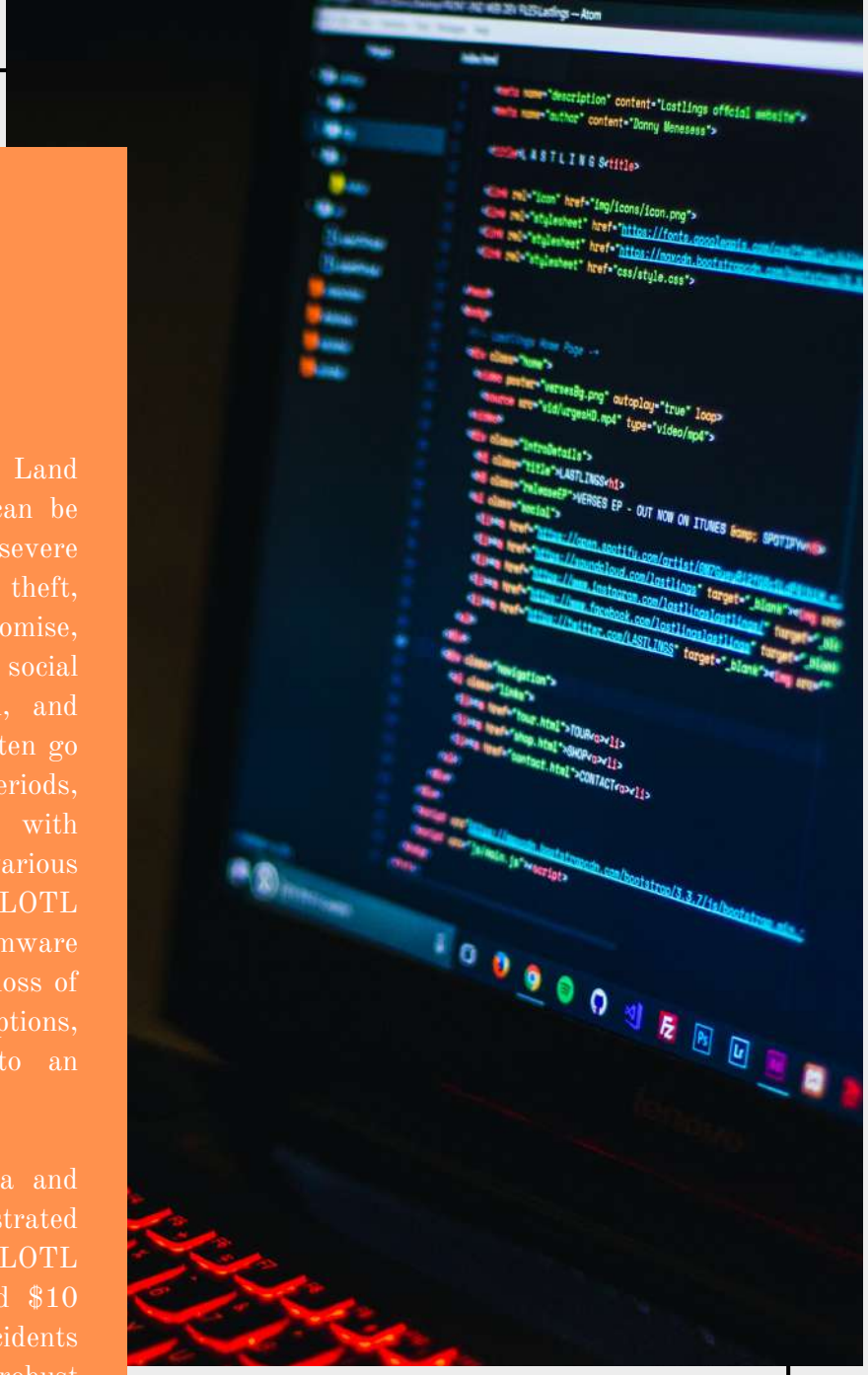
LOTL attacks operate in a fileless manner. This approach eliminates the need for threat actors to implant code directly into the target system to gain access. Recent data from online magazine CSO reveals a staggering 1,400 percent increase in fileless or memory-based attacks leveraging existing software, applications, and protocols over the past year.By mimicking legitimate user actions, LOTL attacks pose a significant challenge for IT teams and security solutions in detecting indications of malicious behavior. This stealthy tactic makes it exceptionally difficult to identify and mitigate the threat promptly.

Protect Against LOTL

1. Regularly monitor network traffic and logs
2. Stay informed on the latest threat intelligence.
3. Leverage behavioral analysis and anomaly detection.
4. Restrict the abuse of legitimate tools.
5. Regularly scan and patch vulnerabilities.
6. Give us a call!

ONECLICKFIX

Amy's Corner: Impact of LOTL Attacks



The impact of Living Off The Land (LOTL) attacks on businesses can be profound, leading to severe consequences such as data theft, extortion, system compromise, sabotage, espionage, fraud, social engineering, privilege escalation, and credential theft. These attacks often go undetected for extended periods, providing cybercriminals with opportunities to carry out various malicious activities. When LOTL attacks transition into ransomware incidents, they can result in the loss of sensitive data, operational disruptions, financial harm, and damage to an organization's reputation.

Notable examples like the Petya and NotPetya attacks in 2017 demonstrated the destructive potential of LOTL techniques, causing an estimated $10 billion in global losses. These incidents highlighted the critical need for robust cybersecurity measures to counter such sophisticated tactics. As LOTL attacks continue to evolve and persist in 2024, it is evident that IT and security teams must enhance their capabilities to identify malicious activities hidden within normal network operations effectively.

ONECLICKFIX

High quality videos online can be used to make fake videos of you doing...whatever...

ONECLICKFIX

WE DO ONSITES OR REMOTES 24 / 7/365

We're there when you need us - onsite or by remote - highly skilled, friendly service that gets it done. We take care of your servers, desktops, laptops, network, internet, and more. Addressing small problems before they become issues. And if your internet goes down, we address it immediately.

ENTERPRISE CIO SERVICES

Have an issue? Let us know, instantly, through our email ticketing system or helpdesk phone. We can also receive alerts regarding your various systems in real time. Not only can you treat us just like an internal IT department, but we can act as your CIO. We provide vision and oversight for your IT - making sure you're using it as a competitive advantage, ensuring your projects stay on budget, and helping you become compliant with industry regulations.

CYBER SECURITY CAN SAVE YOU $$$

Cyber security controls don't have to be expensive, and they can actually save you money. When we implement security controls, not only is your data safer, but so are your employees' actions. Having proper controls can help prevent a breach, which shuts most businesses down as they cannot pay the fines or cannot recover from the client-trust impact. Additionally, security controls can lower cyber security insurance costs!