Logpoint Global Services has researched the banking trojan IcedID, which has developed into a gateway for more sophisticated attacks

Nov 17, 2022 14:06 CET

Cyber attackers hiding behind legal threats: A deep-dive into the IcedID gateway to sophisticated cyberattacks

- **Logpoint Global Services has researched the banking trojan IcedID, which has developed into a gateway for more sophisticated attacks**
- **IcedID leverage legitimate infrastructure like contact forms and email to deliver fake legal threats or spoofed invoices**

COPENHAGEN, Denmark & BOSTON, November 17, 2022 – The threat of a lawsuit can make anyone anxious. And if the threat includes a link to the

evidence, who wouldn't have the urge to click it and see the so-called proof behind the allegation? Unfortunately, that's when the trap snaps shut. The IcedID malware downloads, and adversaries can remotely control the compromised device.

Logpoint Global Services has investigated the IcedID banking trojan by analyzing samples from online sandboxes for its latest installment of the Emerging Threats Protection Report. The report reveals that IcedID has diverse delivery methods, adding legal threats and spoof invoices to social engineering tactics. In addition, IcedID has a complicated behavior. It has developed from a simple banking trojan into a gateway for more sophisticated and harmful cyberattacks. In fact, IcedID is now the second most widespread ransomware family trend, only surpassed by Emotet.

"IcedID is the perfect example of how cybercriminals develop their sophisticated strategies while still using a traditional malware payload to reach their goals," says Doron Davidson, VP Logpoint Global Services. "The ability to detect IcedID is crucial to prevent ransomware attacks and stop a breach before any major damage is done."

To safeguard your organization against IcedID, Doron Davidson recommends:

- Expert monitoring is especially critical in detecting this campaign, given the delivery method and the nature of the malicious emails
- Using in-house social engineering attack scenarios, user awareness training, and empowering employees to recognize and report these attacks will be crucial steps to effectively stop IcedID or any ransomware attacks
- Automation of the incident response increases the chances of shutting down a ransomware attack before important data gets encrypted

Read Logpoint's blog post about the findings here, and access the full Emerging Threats Protection Report, IcedID - Hunting, Preventing, and Responding to IcedID Malware Using Logpoint. The report offers in-depth vulnerability analysis, means to detect and respond to the threat, and insights about incident investigation and response.

Logpoint Global Services is a team of experts who provide cutting-edge

security research in publicly available reports at no cost. As part of the paid service, customers get tailored detection rules, and investigation and mitigation playbooks for recent threats.

About Logpoint

Logpoint safeguards society in a digital world by helping customers and Managed Security Service Providers (MSSPs) detect cyberattacks. Combining reliable technology with a deep understanding of cybersecurity challenges, Logpoint makes security operations easier, giving organizations the freedom to progress. Logpoint's SIEMand NDRtechnologies improve visibility and give a multi-layered approach to cybersecurity that helps customers and MSSPs in Europe navigate the complex threat landscape. Headquartered in Copenhagen, Denmark, Logpoint has a European foundation and is the only European SIEM vendor with a Common Criteria EAL3+ certification. This demonstrates Logpoint's strong focus on data protection and cybersecurity regulations. For more information, visit http://logpoint.com.

Contacts

Maimouna Corr Fonsbøl
Press Contact
Head of PR
PR & Communications
mcf@logpoint.com
+45 25 66 82 98