Lumen Newsroom

DENVER, July 1, 2020 /PRNewswire/ -- Point-of-Sale (POS) malware is nothing new, and the Alina malware – which cyber criminals use to scrape credit card numbers from POS systems – has been around for many years. New intelligence from CenturyLink's Black Lotus Labs, however, revealed that criminals are not yet done with Alina, and they continue to find new ways to use it to steal unsuspecting victims' credit- and debit-card data.

The theft was discovered after one of Black Lotus Labs' machine-learning models flagged unusual queries to a specific domain in April 2020. Rigorous research determined that the Alina POS malware was utilizing Domain Name System (DNS) – the function that converts a website name into an IP address – as the outbound communication channel through which the stolen data was exfiltrated.

"Black Lotus Labs is releasing this intelligence in support of our mission to leverage our global network visibility to protect our customers and keep the internet clean," said Mike Benjamin, head of Black Lotus Labs. "We will continue to monitor this situation as we work to eliminate the threat. We strongly recommend that all organizations monitor DNS traffic for suspicious queries to prevent this and other threats."

**The Bottom Line:**

POS malware continues to pose a serious security threat, and DNS is a popular choice for malware authors to bypass security controls and exfiltrate data from protected networks. Malicious actors regularly update their Tactics, Techniques and Procedures (TTPs) to evade detection, so the best defense is continuous monitoring for anomalous behavior.

**Details Of Black Lotus Labs' Findings Can Be Found in the Alina POS Malware Blog: https://blog.centurylink.com/alina-point-of-sale-malware-still-lurking-in-dns**

**How and Why DNS is Important:**

Credit card processing systems typically run in Windows environments, allowing them to be targeted by the existing skills of the crimeware markets. Although credit card processing occurs in highly restricted environments, DNS often goes unmonitored, which makes it an attractive choice for the exfiltration of credit card information.

To do this, malware authors encode the stolen information and issue a DNS query to the actor-controlled domain name. The encoded data is placed in a subdomain, which the malicious actors then extract when they receive the DNS query. The stolen data is subsequently sold in underground criminal markets.

**Key Research Findings:**

- This POS malware uses DNS to evade detection and bypass security controls.
- Four domains showed similar DNS queries. A suspicious looking fifth domain was unused, but it was hosted on the same IP. Actors often register multiple domains to provide redundancy if one or more of the malicious domains is blocked.
- Black Lotus Labs was able to identify Alina's encoding methodology and confirm exfiltration

of the stolen data.

**Additional Resources:**

- Learn more about Black Lotus Labs: **https://centurylink.com/blacklotuslabs**
- Read more about DNS threats in the CenturyLink 2019 Threat Research Report: **https://www.centurylink.com/asset/business/enterprise/report/2019-threat-research-report.pdf**
- Read our blog on Ismdoor malware and the use of DNS tunneling: **https://blog.centurylink.com/ismdoor-malware-continues-to-make-use-of-dns-tunneling/?utm_source=black%20lotus%20labs&utm_medium=referral**

**About CenturyLink:**

CenturyLink (NYSE: CTL) is a technology leader delivering hybrid networking, cloud connectivity, and security solutions to customers around the world. Through its extensive global fiber network, CenturyLink provides secure and reliable services to meet the growing digital demands of businesses and consumers. CenturyLink strives to be the trusted connection to the networked world and is focused on delivering technology that enhances the customer experience. Learn more at **http://news.centurylink.com/**.

SOURCE CenturyLink Inc.

For further information: Suzanne K. Dawe, CenturyLink, (318) 582-7011, suzanne.dawe@centurylink.com

---

**https://news.lumen.com/2020-07-01-New-Intelligence-Reveals-that-Alina-Point-of-Sale-Malware-is-Still-Lurking-in-DNS**