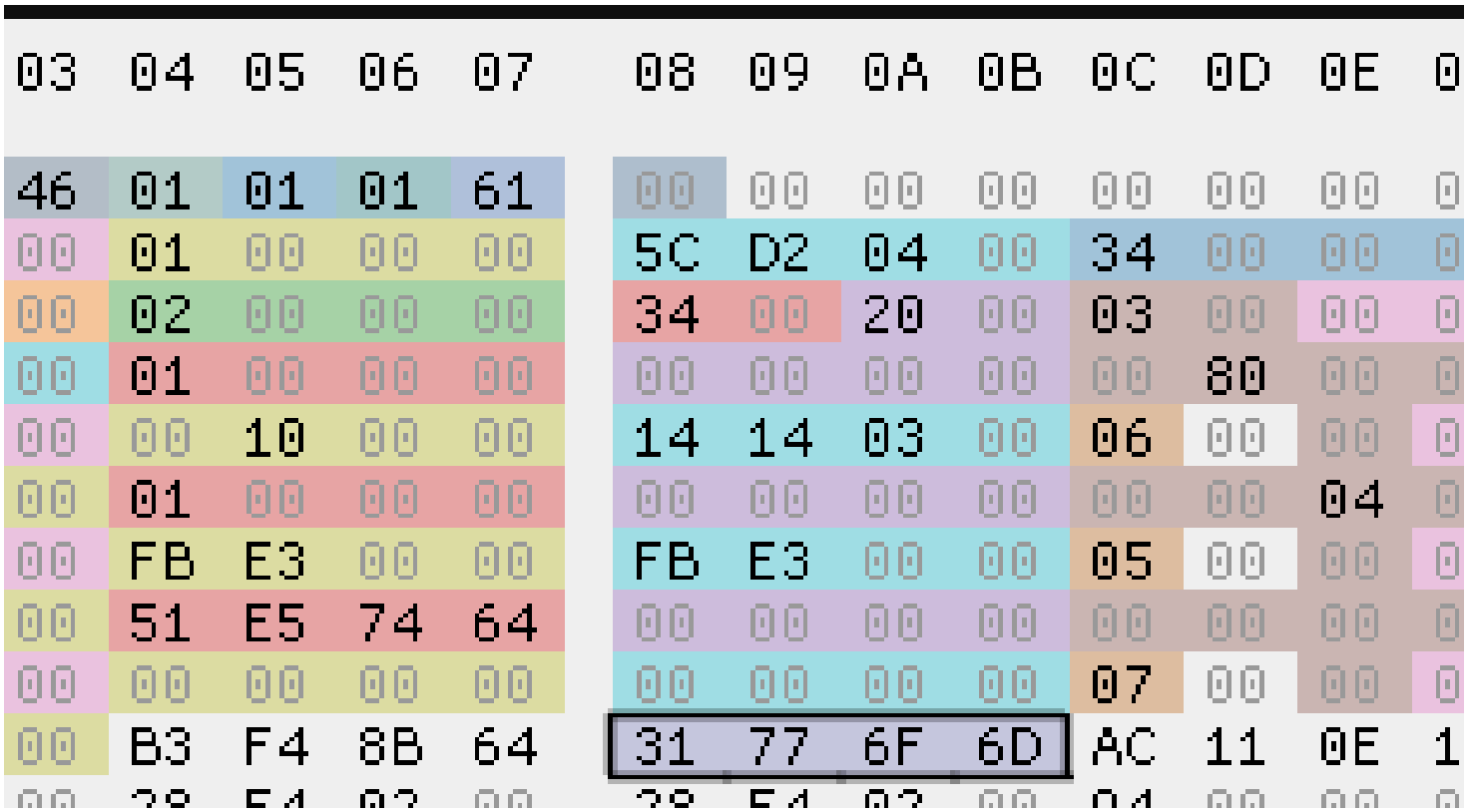
EN

A collection of 16 posts



EN

Gayfemboy: A Botnet Deliver Through a Four-Faith Industrial Router 0-day Exploit.

Overview Countless script kiddies, dreaming of getting rich, rush into the DDoS black-market industry armed with Mirai source code, imagining they can make a fortune with botnets. Reality,...

2025年1月7日 · 9 min read

APT

New Zero-Detection Variant of Melofee Backdoor from Winnti Strikes RHEL 7.9

Background On July 27, 2024, XLab's Cyber Threat Insight and Analysis System(CTIA) detected an ELF file named pskt from IP address 45.92.156.166. Currently undetected on VirusTotal, the file triggered two alerts: an Overlay section and a communication domain mimicking Microsoft. Our...

2024年11月12日 · 6 min read

Botnet

Uncovering DarkCracks: How a Stealthy Payload Delivery Framework Exploits GLPI and WordPress

Summary XLab's Cyber Threat Insight and Analysis system(CTIA) recently detected a sophisticated malicious payload delivery and upgrade framework, which we have named DarkCracks. This...

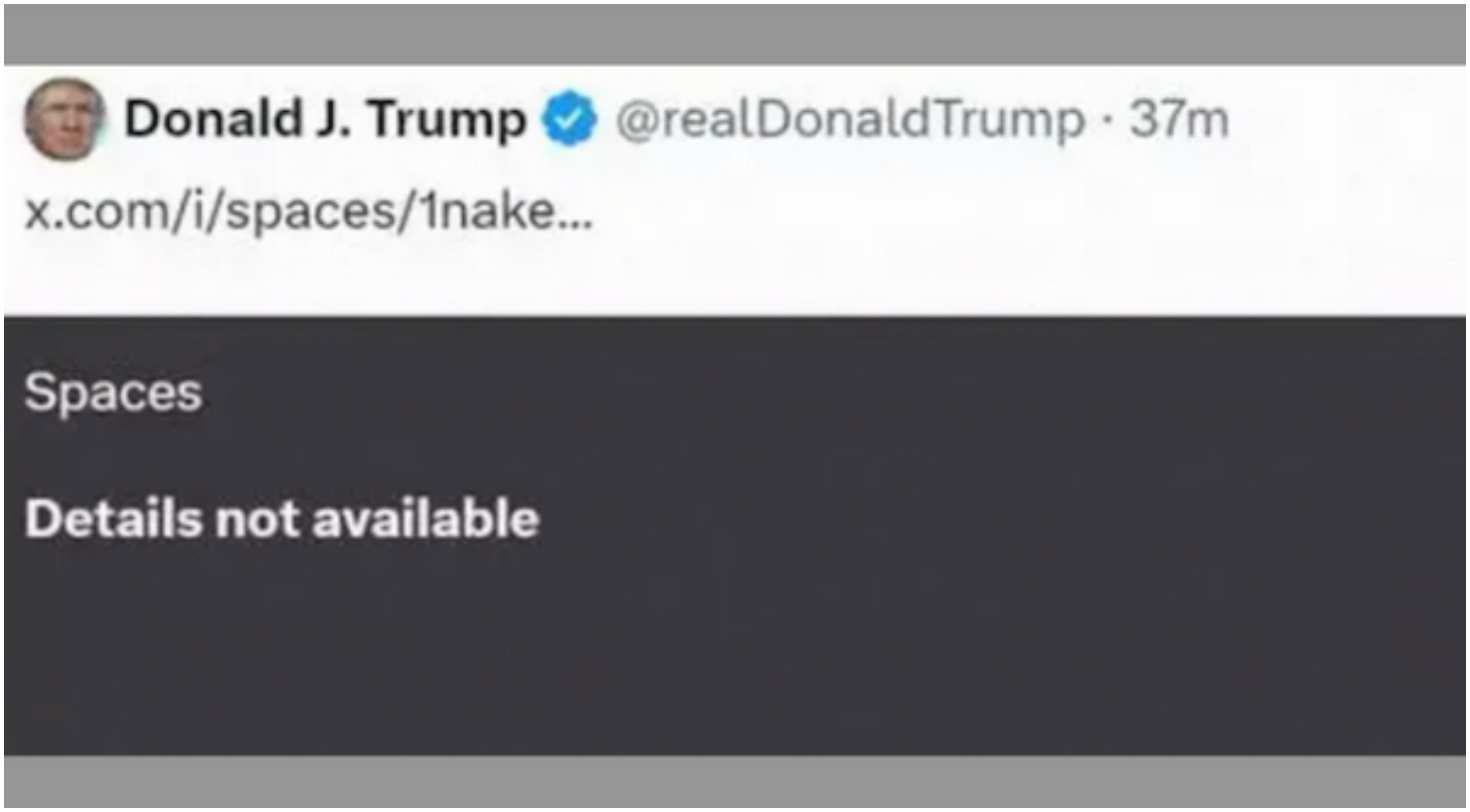
2024年9月4日 · 22 min read

DDoS

More details on the DDoS attack on the 《Black Myth: Wukong》 distribution platform

Incident Review On the evening of August 24th, Steam platform suddenly went down, with players around the world reporting that they were unable to log in. Many players speculate that the crash i...

2024年8月29日 · 11 min read



DDoS

Behind the Scenes: A Brief Overview of the DDoS Attack on the Trump-Musk Livestream

Note: There has been considerable discussion in both the media and the security community about whether the Trump and Musk interview livestream on X yesterday was indeed the target of a DDo...

2024年8月14日 · 3 min read

Backdoor

8220 Mining Gang's New Tool: k4spreader

Overview On June 17, 2024, we discovered an ELF sample written in C language with a detection rate of 0 on VT. This sample was packed with a modified upx packer. After unpacking, another...

2024年6月25日・9 min read

DDoS

New Threat: A Deep Dive Into the Zergeca Botnet

Background On May 20, 2024, while everyone was happily celebrating the holiday, the tireless XLab CTIA(Cyber Threat Insight Analysis) system captured a suspicious ELF file around 2 PM, located a...

2024年6月19日 · 13 min read

EN

Breaking Network Boundaries with SSH Services

Background Recently, XLab received a project that requires the deployment of a self-developed system on a restricted intranet. Due to objective constraints, we are unable to directly access their intranet. Initially, we planned to use "Sunlogin(Remote Control Tool)" as a solution, but the networ...

2024年5月31日 · 6 min read

Packer

Kiteshield Packer is Being Abused by Linux Cyber Threat Actors

Background Over the past month, XLab's CTIA(Cyber Threat Insight Analysis) System has captured a batch of suspicious ELF files with low detection rates on VT and very similar characteristics....

2024年5月28日 · 8 min read

Botnet

CatDDoS-Related Gangs Have Seen a Recent Surge in Activity

Overview XLab's CTIA(Cyber Threat Insight Analysis) System continuously tracks and monitors the active mainstream DDoS botnets. Recently, our system has observed that CatDDoS-related gang...

2024年5月22日・8 min read

Backdoor

Playing Possum: What's the Wpeeper Backdoor Up To?

Summary On April 18, 2024, XLab's threat hunting system detected an ELF file with zero detections on VirusTotal being distributed through two different domains. One of the domains was marked as...

2024年4月29日 · 11 min read

DDoS

Smargaft Harnesses EtherHiding for Stealthy C2 Hosting

Background At XLab, we see a lot of botnets every day, mainly tweaks of old Mirai and Gafgyt codes. These are pretty common and usually don't grab our attention. But today, we found...

2024年2月2日 · 16 min read

DNS

Deep Dive into NXDOMAIN Data in China

The Domain Name System (DNS) is an essential protocol in the architecture of today's Internet. It routinely translates domain names into IP addresses and also often handles a multitude of invalid...

2024年1月29日・32 min read

Botnet

Bigpanzi Exposed: The Hidden Cyber Threat Behind Your Set-Top Box

Background Some time ago, we intercepted a dubious ELF sample exhibiting zero detection on VirusTotal. This sample, named pandoraspear and employing a modified UPX shell, has an MD5...

2024年1月15日 · 33 min read

Botnet

Rimasuta New Variant Switches to ChaCha20 Encryption Algorithm

In June 2021, 360netlab discovered a completely new variant of the Mirai malware. It was named Mirai_ptea based on the use of the TEA algorithm. However, the author of the malware expressed dissatisfaction in subsequent samples after the variant was publicly disclosed to the community: ...

2024年1月10日 · 12 min read

Botnet

Mirai.TBOT Uncovered: Over 100 Groups and 30,000+ Infected Hosts in a big IoT Botnet

Overview As we all know Mirai was first discovered in 2016 and it infects IoT devices by exploiting their weak passwords and vulnerabilities. Once the devices are infected, they become part of a botnet controlled by attackers for large-scale distributed denial-of-service attacks. Mirai botnets...

2024年1月3日 · 13 min read