Cisco
Security

Cisco Theater Presentation Schedule

Cisco
Security

Cisco Theater
Presentation Schedule

An inside look into PDF phishing trends in 2024

Wed 10:30am

In 2024 PDF remains one of the most abused document formats to deliver phishing content via email attachments. QR code phishing, call-back and click-through scams are among the most prevalent techniques used by attackers to evade security solutions and steal user credentials. During the presentation we will deep-dive into some recent PDF samples found in the wild and the techniques that Talos has developed to analyze and block them.

Data Exfiltration: MFT analysis of Rclone

Wed 11:00am

Open-source tools, such as Rclone, are often abused by threat actors, such as the Akira and BlackBasta ransomware operations, to exfiltrate data from compromised environments. Threat actors are known to remove configuration files to cover their tracks, making it challenging for organizations to identify what data was stolen. Through the analysis of the Master File Table (MFT) in a Windows environment, organizations can gain insight into what may have been exfiltrated using Rclone. This talk will discuss these techniques and demonstrate how to effectively analyze the MFT to uncover data exfiltration activities.

SnortML Talk

Wed 11:30am   Thur 2:00pm

SnortML is a machine learning-based detection engine capable of detecting zero-day attacks fitting known vulnerability types. SnortML identifies when payloads match a particular vulnerability class, even if there are variations, allowing customers to get in front of the fight against zero-day attacks.

Vulnerability Discovery Year in Review

Wed 1:00pm

Overview of vulnerabilities discovered by the Vulnerability Discovery and Research team in the past year.

Fuzzing Android Apps With Frida and AFL++

Wed 1:30pm

Overview of finding memory corruption vulnerabilities in native code of proprietary 3rd party Andoid applications using Frida and AFL++.

Integrating Snort into Splunk

Wed 2:00pm

With Cisco's recent acquisition of Splunk, there is a large opportunity for integration of IPS/IDS event feeds into the Splunk analytical platform. Come see how we combine two technologies to enrich your security event data.

Hunting Black Basta through DNS

Wed 2:00pm

Following a Black Basta attack through DNS query logs. We'll inspect the tunneling/exfiltration behaviors across infected clients. (product relevance is Secure Access or Umbrella)

Security events for the rest of us: A look at commonly encountered alerts

Wed 3:00pm   Thur 3:00pm

Being able to pull data from 550 billion daily security events presents a great opportunity for uncovering new and novel attack techniques and campaigns. But in a data set of this size these are a minority–the needles in a haystack of security events. What's contained in the rest of this data is often what your average security practitioner is dealing with in the day-to-day grind. In this talk, we'll examine several Cisco telemetry sources to answer the question "what types of events are security practitioners likely to encounter in the current threat landscape?"

All bins are lolbins on Linux

Wed 3:30pm

Overview of linux process model and unix philosophy and how it naturally leads to attackers and sysadmins using the same tools for various tasks.

Initial Infections: A history

Wed 4:00pm

Taking a look at ways attackers perform their initial infections on their victims. Will be mostly centered around data showing how attackers pivoted from using Microsoft Office Macros to different TTPs following Microsoft disabling macros by default in May of 2024. Will be using data from Corpus to show data trends of malicious attachments.

Exploring Infostealer TTPs on Automotive Head Units

Wed 4:30pm

Automotive vehicles have become exponentially more computerized in the last decade, and automakers continue to add new functionality and integrations to these systems. While most research focuses on the safety features of autonomous and semi-autonomous vehicle capabilities, there is little research regarding the data collected by these systems and whether this data is of interest to threat actors. By exploring exposed data, pivot points, and user impact, automakers and drivers can benefit from understanding how they can better protect themselves from unwanted data exposure and potential malware. The research conducted focuses on threat modeling a sampled Android-based infotainment system, ascertaining what data could be of interest to a financially motivated threat actor, and identifying techniques to demonstrate impact.

Ransomware trends, 2023-2024

Wed 5:00pm

This talk will leverage the results of our team's massive research effort on ransomware in support of Cisco's MITRE 6 testing efforts this year. Based on a comprehensive analysis of the top 14 most active ransomare groups between 2023 and 2024, we found commonalities/ differences across actors, top TTPs observed, and constructed a typical ransomware attack chain. This talk will also touch on why these findings still matter today, including actors' focus on edge devices (which we've written about on the blog and which non-ransomware actors like Volt Typhoon are also known to target // general awareness, etc.).

The Threat Intel / DFIR ecosystem: How one supports the other

Wed 5:30pm

The collaboration between digital forensics and incident response (DFIR) and cyber threat intelligence (CTI) teams can enhance an organization's ability to comprehensively understand and respond to a multitude of cyber threats. Proactive and actionable intelligence can lead DFIR teams to the "right place to look" while forensic efforts can provide valuable information for CTI teams, which can help with tracking various threats. Cisco Talos Incident Response team regularly collaborates with the Talos Intelligence and Interdiction teams to provide customers with the best analysis and outcomes during incident response investigations. During this presentation, we will cover the importance of the relationship between DFIR and CTI teams.

The rise of Loader for malware delivery

Thur 10:30am

This talk will focus on the rise of loader and technique improvisation like obfuscation, persistence, defense evasion for malware delivery. Loaders have been used for a long time, however, their use recently shows an upward trend due to its easy application to deliver infostealer, ransomware and other malware.

Striving towards the text tokenization endgame

Thur 11:00am

Text is a domain which has been extensively pursued in machine learning, however it has always required processing the raw data into a form more representable by models. One upside of text is that it often presents opportunities to first learn models directly from the data, later applying what we've learned for more targeted classification tasks where we may not have as much labeled data as raw data. This talk will review several major steps in the representation of text and associated unsupervised techniques (BoW/tfidf, word2vec, subword tokens), showing how at each step more computationally intensive techniques have increased the representative capacity of models and unlocked new applications for them, and how they've tried to overcome the limits of the previous approaches. The talk will conclude by covering an area of my research on character level representations and how they can be applied to even the most challenging kinds of text data (for instance non-natural language strings found in email), with the broader narrative theme that by representing text at the individual character level we have reached the last stage of text tokenization approaches as characters are the foundational component of text.

Different Victims, Same Layout: Insights into Email Kit Reuse in the Wild

Thur 11:30am

This talk will unveil the pervasiveness of email kit reuse in the wild. We will present concrete example emails our customers receive that have similar or identical email templates. We will also explain the differences between email kits and phishing kits. It will be discussed what problems email kit reuse can create for existing email security products that rely on reputation services, detection rules, and even advanced ML-based solutions. We will conclude the talk by proposing some solutions as future work.

Snapshot fuzzing macOS

Thur 1:00pm

Using a snapshot-based approach enables us to target closed-source code without custom harnesses precisely. Researchers can obtain full instrumentation and code coverage by executing tests in an emulator, which enables us to perform tests on our existing hardware. While this approach is limited to testing macOS running on Intel hardware, most of the code is still shared between Intel and ARM versions.

Heap shaping and data visualization

Thur 1:30pm

Modern exploitation often requires manipulating the heap via innocuous operations in order to create a layout that will then be leveraged during the actual heap exploitation stage. Whether it is from an attacker perspective to create an exploit, or from an analyst perspective to understand how an in the wild exploit operates, it can be beneficial to be able to visualize these heap operations during the heap shaping process. This talk will briefly touch on how these primitives operates and then share how to use dynamic binary instrumentation (e.g. FRIDA, WinDBG) to log these memory allocations and visualize the result with some simple graphic programming methods.

Usable Data

Thur 2:30pm

Making data usable in pipelines and databases for various skill levels to enable hunting and automation. Avoid common pitfalls and corner-cuts that come back to bite you.

Dark side of the generative AI: impersonations, scams, sextortions

Thur 3:30pm

Overview and examples of novel attacks which are powered by generative AI.

Cisco
Security

Cisco Theater Presentation Schedule

Wednesday, August 7th

10:30am	An inside look into PDF phishing trends in 2024
11:00am	Data Exfiltration: MFT analysis of Rclone
11:30am	SnortML Talk
1:00pm	Vulnerability Discovery Year in Review
1:30pm	Fuzzing Android Apps With Frida and AFL++
2:00pm	Integrating Snort into Splunk
2:30pm	Hunting Black Basta through DNS
3:00pm	Security events for the rest of us: A look at commonly encountered alerts
3:30pm	All bins are lolbins on Linux
4:00pm	Initial Infections: A history
4:30pm	Exploring Infostealer TTPs on Automotive Head Units
5:00pm	Ransomware trends, 2023-2024
5:30pm	The Threat Intel / DFIR ecosystem: How one supports the other

Thursday, August 8th

10:30am	The rise of Loader for malware delivery
11:00am	Striving towards the text tokenization endgame
11:30am	Different Victims, Same Layout: Insights into Email Kit Reuse in the Wild
1:00pm	Snapshot fuzzing macOS
1:30pm	Heap shaping and data visualization
2:00pm	SnortML Talk
2:30pm	Usable Data
3:00pm	Security events for the rest of us: A look at commonly encountered alerts
3:30pm	Dark side of the generative AI: impersonations, scams, sextortions

cisco