

ICE22

Activity Clustering: Tracking the Actors Behind the Threats

Josh Davies – Product Manager

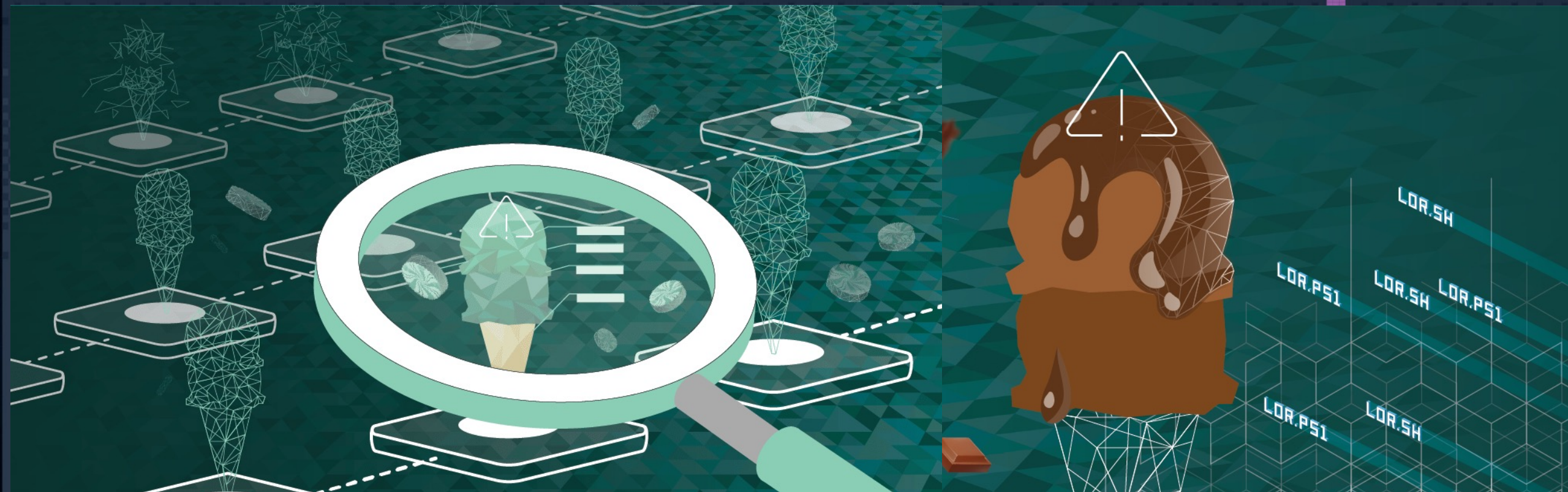
Project Ice Cream

Unique Insight

Into 4000+ Customers producing
a 30Pb threat data lake

To Create

Activity clusters of known
threat actors / groups



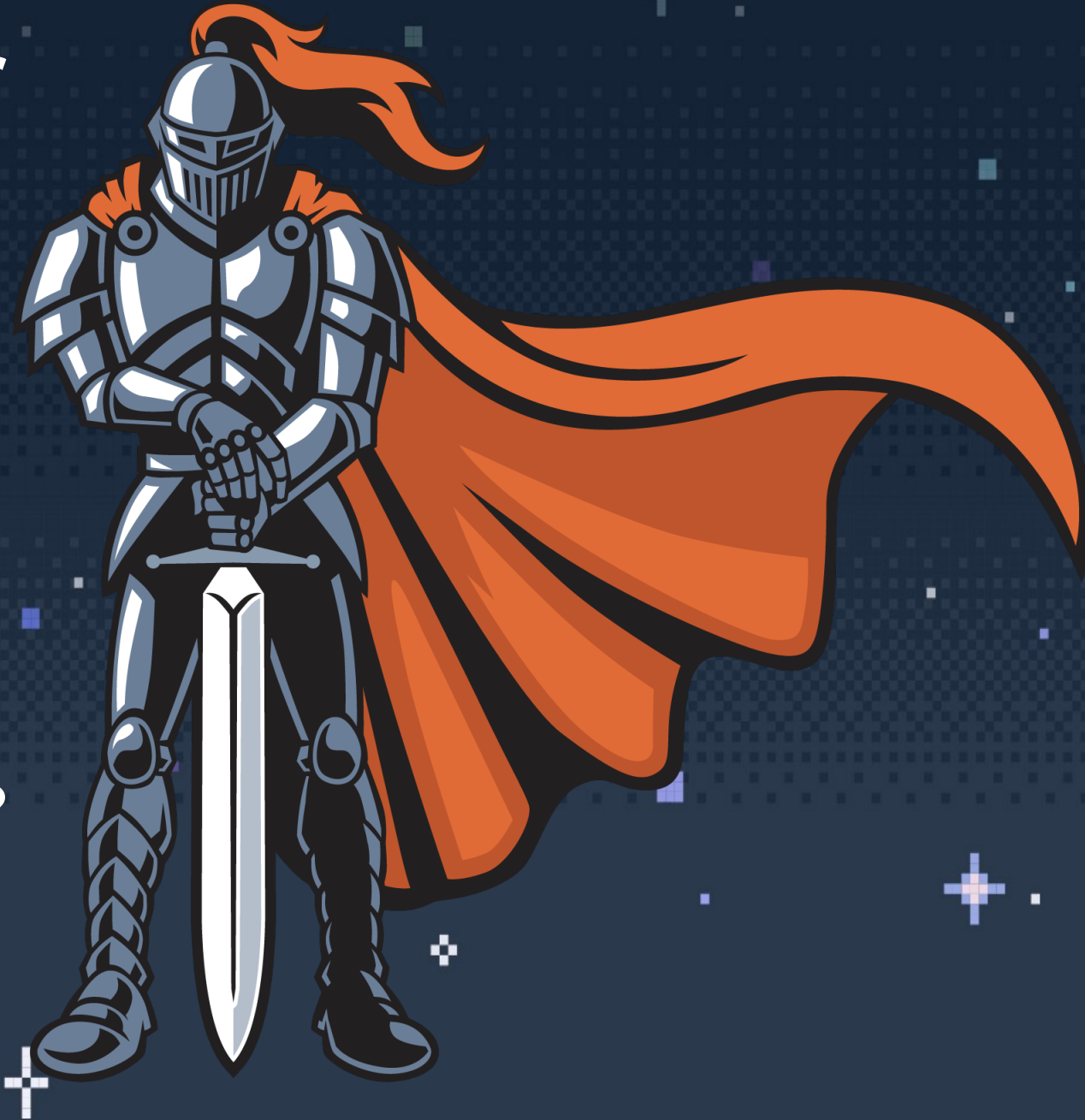
Threat vs Threat Actor

Threat

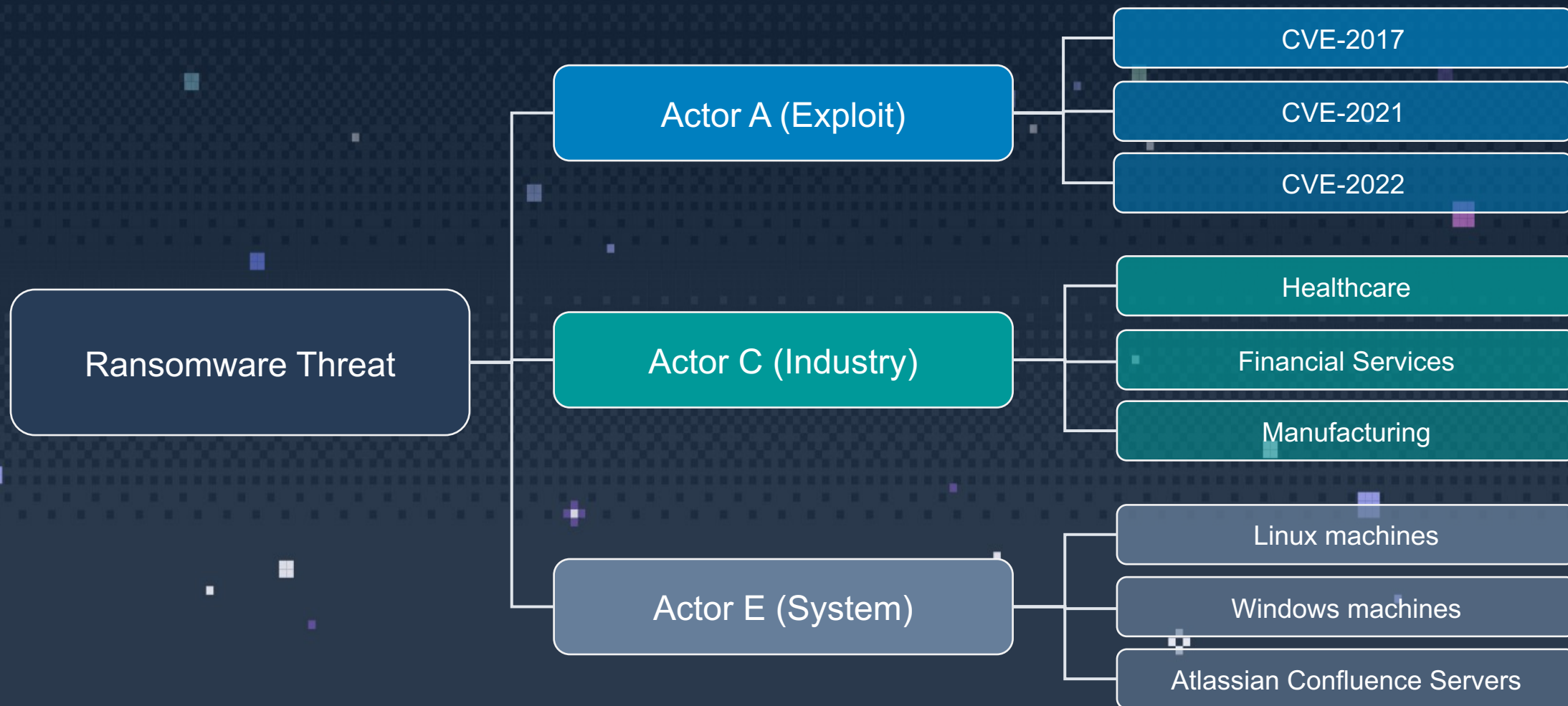
The weapon(s) used to achieve objectives

Threat Actor

The person(s) behind the threats
Who? What? Why? How? Where?



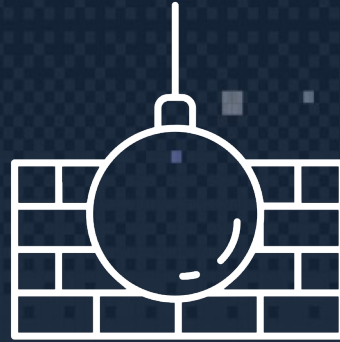
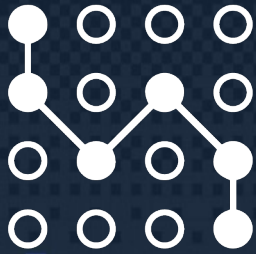
Threat to Actor to Campaign





Battle of Pelusium by Simon Seitz for World History Encyclopedia.

Analysis Methodology



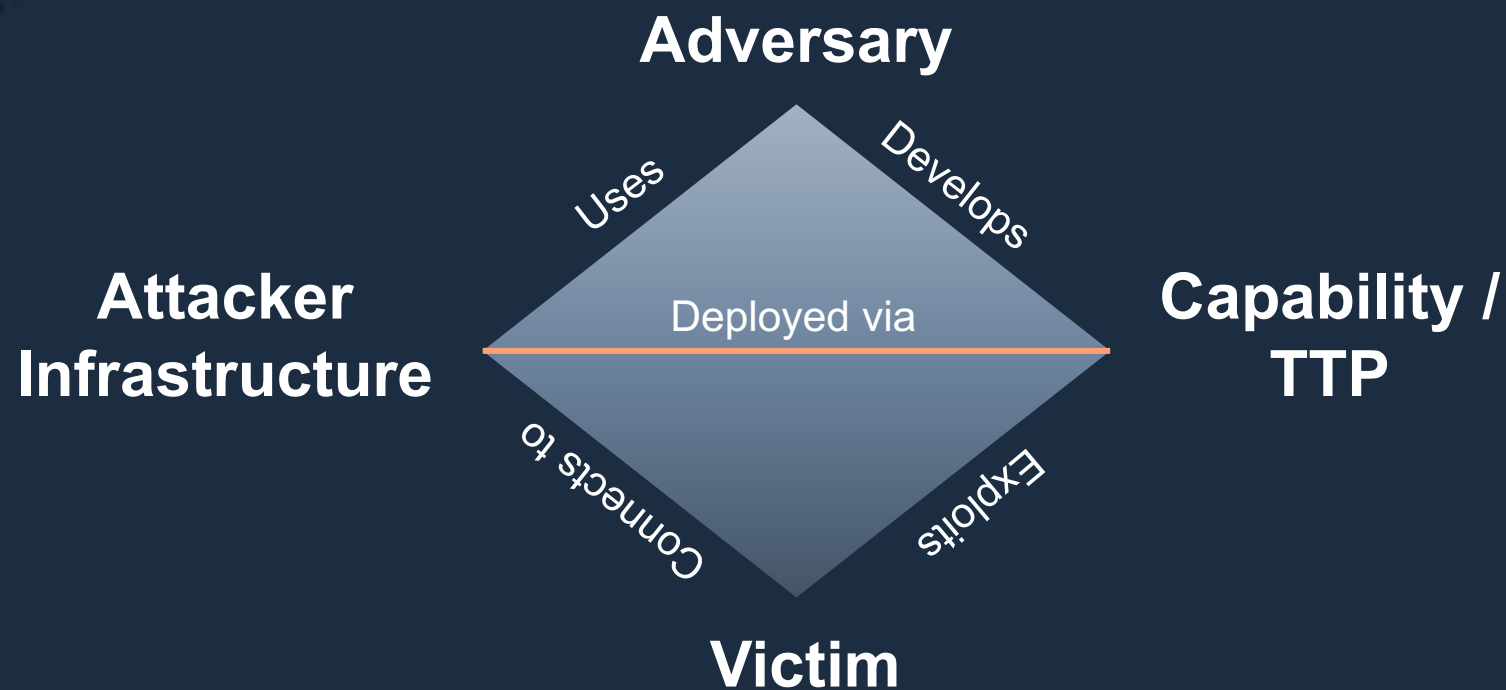
Cyber Kill
Chain

MITRE
ATT&CK

Diamond
Model

The Diamond Model

Clustering activity under a single threat group or adversary to better track and detect their actions.



Mint Example

Recon

Exp

Inst

C2

AoO



Kill Chain



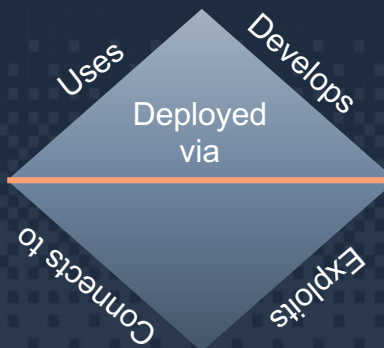
ATT&CK



PINDC-AS [recon]
RMINJINERIN [recon]
SELECTEL [recon]
EUROBYTE Eurobyte LLC [exp]
Hosting vpsville[.]ru [exp]
IHOR-AS [exp]
BEST-HOSTER [inst]
EUROBYTE Eurobyte LLC [inst]
ITLAS [inst]
EUROBYTE Eurobyte LLC [C2]
GREENFLOID-AS [C2]
ITEXPRESS-AS [C2]
ASBAXET [AoO]
FLYNET-AS [AoO]

Attacker
Infrastructure

Adversary



Capability
/ TTP

Active Scanning - T1595 [recon]
Exploit Public-Facing App - T1190
[recon/delivery/exploit]
Scheduled Task/Job: Cron - T1053.003
[inst persistence]
Ingress Tool Transfer - T1105 [inst / C2]
Application Layer Protocol - T1071 [C2]
Resource hijacking - T1496 [AoO]

Victim

Exposed & vulnerable servers
Linux

Mint's Campaigns

PHP Eval
CVE-2017-9841

Citrix RCE
CVE-2019-19781
Think PHP
CVE-2019-9082

SaltStack Authentication Bypass
CVE-2020-11651
Liferay
CVE-2020-7961
BIG-IP TMUI RCE
CVE-2020-5902
MobileIron Core & Connector
CVE-2020-15505
Web Logic
CVE-2020-14882/CVE-2020-14750
Micro Focus
CVE-2020-11854

Laravel Ignition
CVE-2021-3129
Confluence
CVE-2021-26084
Apache RCE
CVE-2021-41773

Confluence
CVE-2022-26134
F5 BIG-IP
CVE-2022-1388
Spring4Shell
CVE-2022-22965

2017

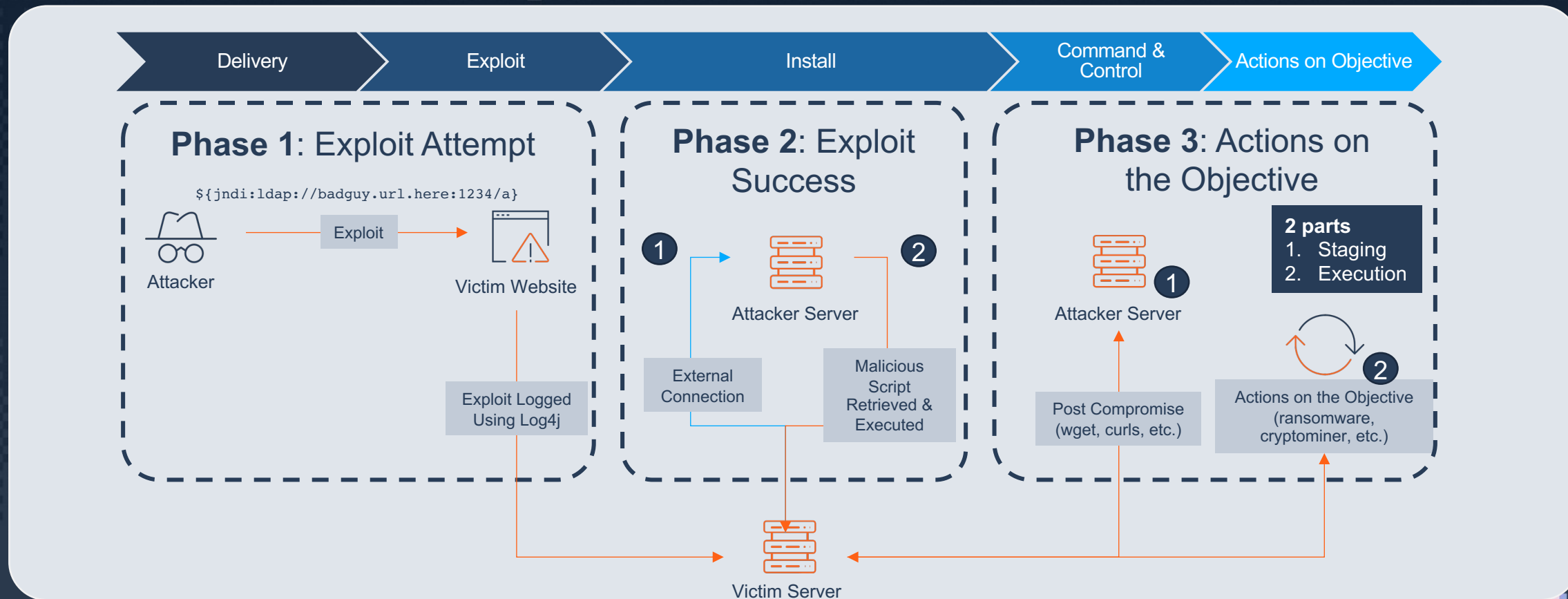
2019

2020

2021

2022

Layers of Defense: Log4Shell Attack Flow



Block
Detect
Telemetry

WAF
Log Analysis, IDS
Nginx, Apache, IIS,

Firewall Policies
Logs, IDS, FIM

EDR, DLP, AV
UBA, Logs, IDS, FIM

Developments to the Diamond



**Attacker
Infrastructure**

Adversary

Uses

Develops

Deployed via

Connects to

Exploits

Victim

A 5x5 grid of cells. The central cell (row 3, column 3) is red. The four cells immediately adjacent to the center (up, down, left, right) are also red, forming a cross shape. All other cells in the grid are white.



Microsoft Windows
(c) 2019 Microsoft

[illegible]

LICTANIUS nephew to the king

Activity Clustering Outcomes

For Alert Logic

- Understand threat groups behind the threats
- Early warning of zero-days
- Insights of where to look next
- Anticipate next steps




For Organizations

- Better detection
- Better remediation advice
- Quicker response
- Comprehensive response
- Limit impact
- Apply lessons learned

Want to learn more?


Search Alert Logic Threat Intelligence Blogs

Threat Intelligence




SEP 23, 2022

The Botnet Crypto-mining Conquest



SEP 9, 2022

**What's Old is (Sort of) New Again:
Bad Actors Continue Their Love of
Web Shells**



SEP 1, 2022

**Shining a Light on Visibility for
Enhanced Security Posture**

<https://www.alertlogic.com/blog/threat-activity-clusters-project-ice-cream/>



Next Steps

Get a technical deep dive of our solution by requesting a demo from one of our security experts

REAL Ice Cream delivered

