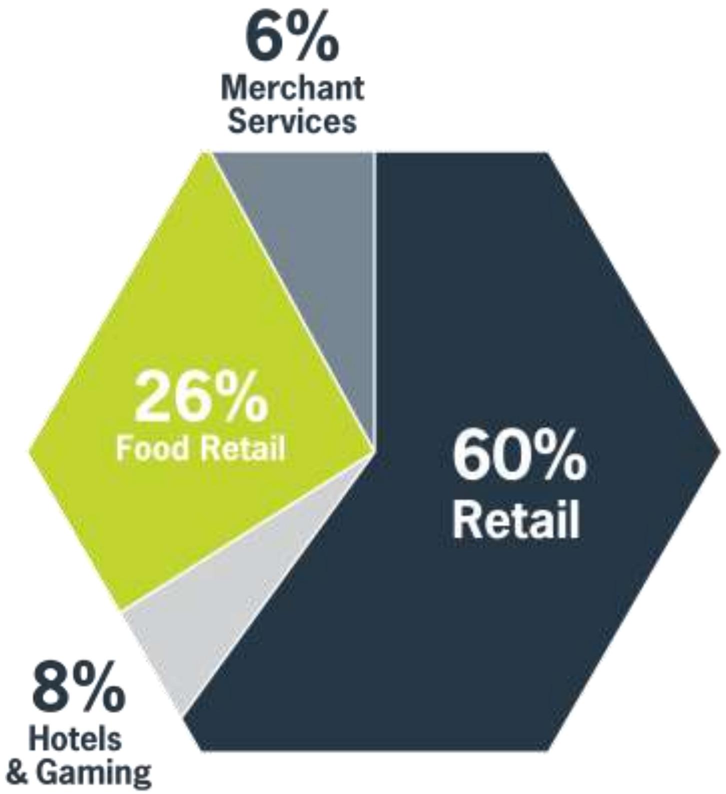
R-CISC

THE RETAIL ISAC

Protect as **ONE.**

Our Mission: Reduce the risk to the retail community by sharing cyber threat intelligence and security best practices.

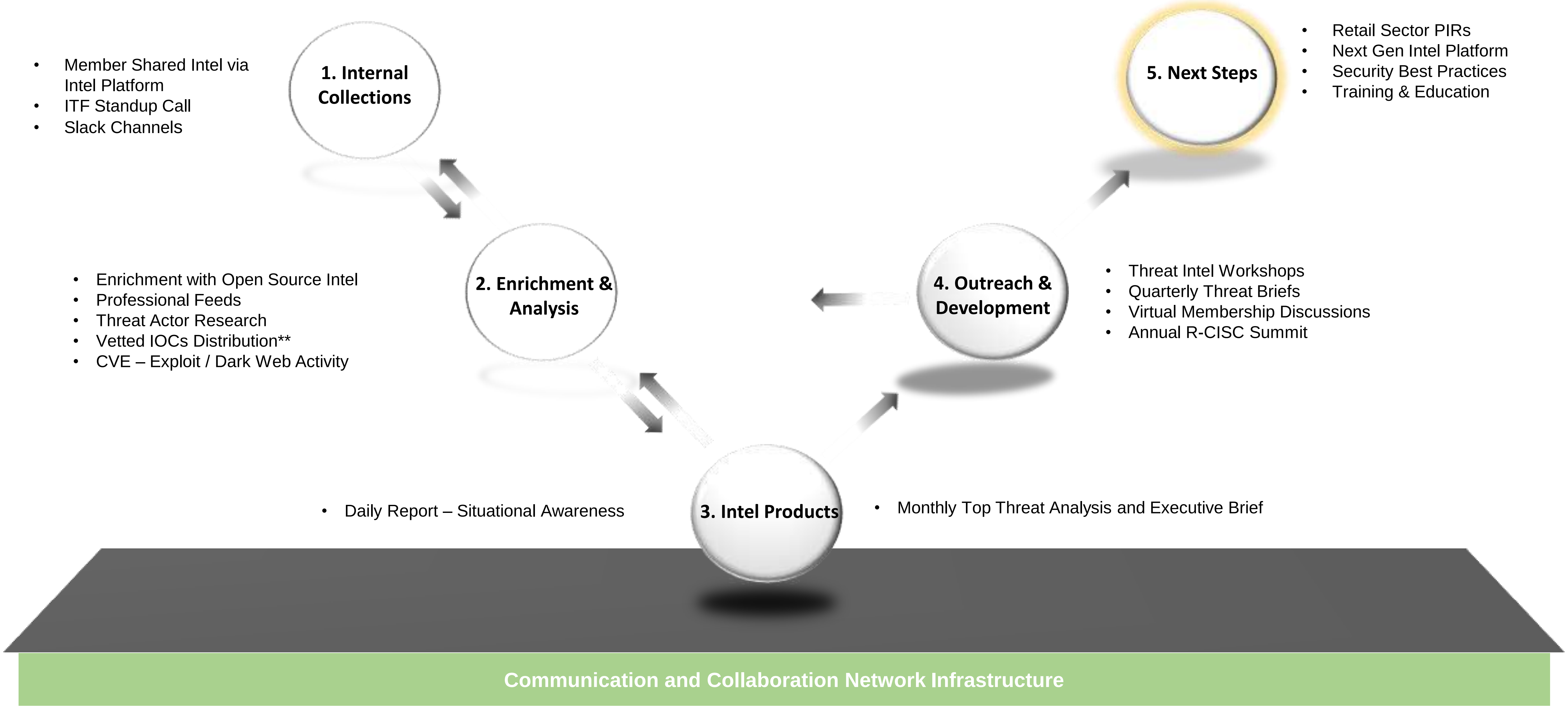


Top Threats

- Phishing (spear-phishing or whaling)
- Credential Stuffing
- Account Take Over (ATO)
- Advanced Persistent Threat (ATP)
- PoS Malware and threats
- Denial of Service
- Ransomware

R-CISC

Operational Model



1. Internal Collections

- Member Shared Intel via Intel Platform
- ITF Standup Call
- Slack Channels

2. Enrichment & Analysis

- Enrichment with Open Source Intel
- Professional Feeds
- Threat Actor Research
- Vetted IOCs Distribution**
- CVE – Exploit / Dark Web Activity

3. Intel Products

- Daily Report – Situational Awareness
- Monthly Top Threat Analysis and Executive Brief

4. Outreach & Development

- Threat Intel Workshops
- Quarterly Threat Briefs
- Virtual Membership Discussions
- Annual R-CISC Summit

5. Next Steps

- Retail Sector PIRs
- Next Gen Intel Platform
- Security Best Practices
- Training & Education

Communication and Collaboration Network Infrastructure

Threat Intel Team

CTI Tactical Analyst

- Interface: Threat Analysts
- IOC Management
- Vulnerability Intel
- Malware & Ransomware Intel
- Phishing, Fraud, ATO
- ID targeted attacks, campaigns
- ID attack phase (kill chain)

Intel Ops Manager

- Interface: Operation Leads
- Detection & Response Strategies
- Blocking & Triage
- Threat Actor Management & TTP
- Monitoring the underground
- Investigation & Attack Analysis
- Daily Situational Awareness

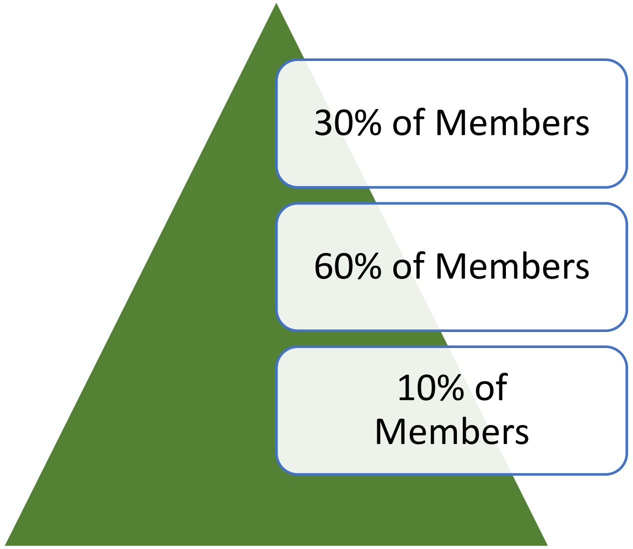
-

Strategic Intel Manager

- Interface : Organizational Leads
- Monthly Threat Analysis Reporting
- Monthly Executive Brief
- Security Alerts
- Align Threats to Business
- Trending & threat forecasting
- Technology reviews
- Threat Intel Security Strategy
- Intel & Security Best Practices

Member Organization Methods for Sharing Threat Intelligence

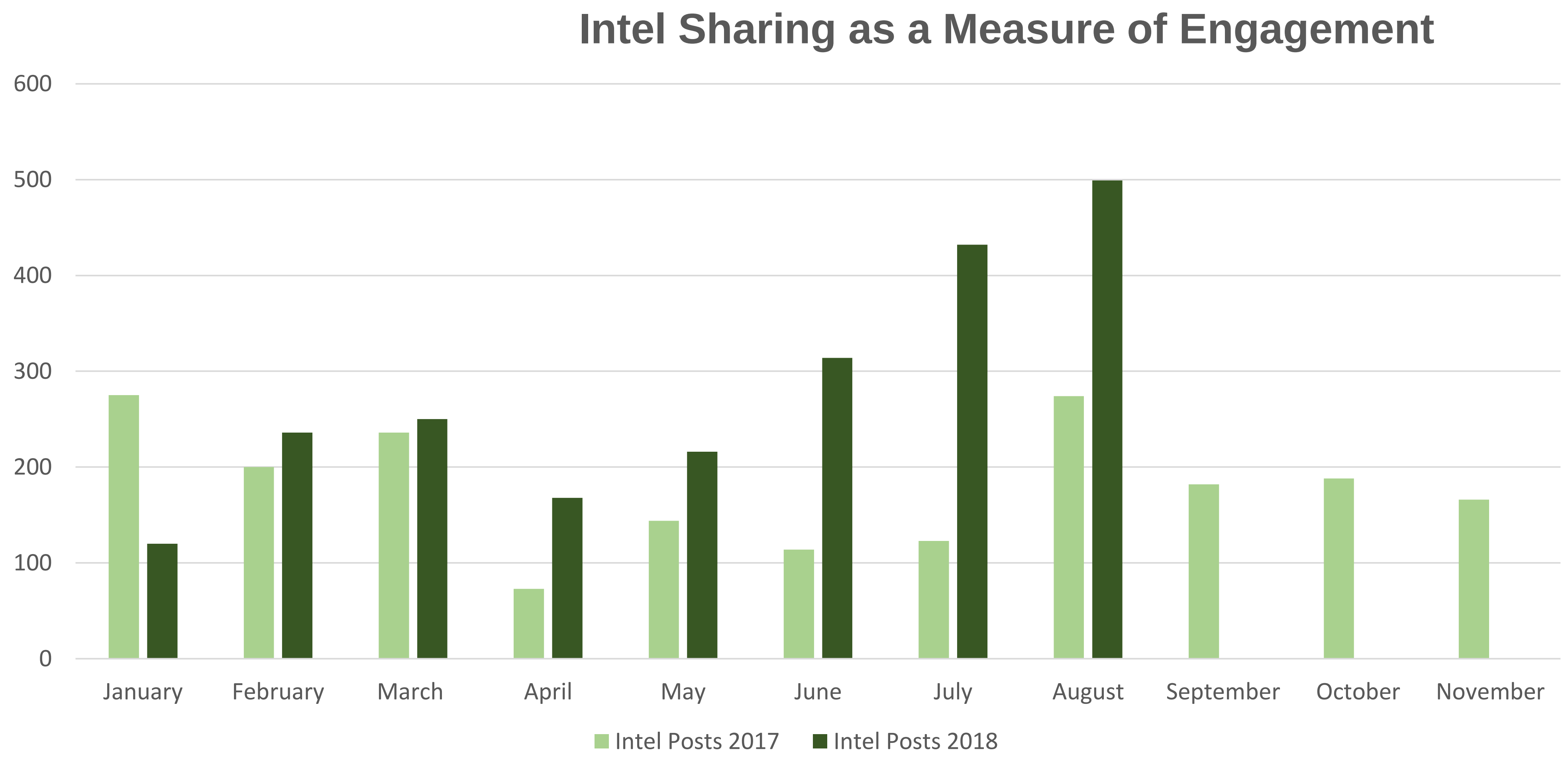
Threat Intel Function	• Core & ITF ListServ Email Distribution • TruSTAR • ITF Calls & Slack
Outsourced Security Services	• Core ListServ Email Distribution • MSSP Intel Share ListServ Email Distribution • TruSTAR (w/access to Vetted Enclave)
No Threat Intel Function	• Core ListServ Email Distribution / TruSTAR • Network layer Data Capture & Intel Sharing



30% of Members

60% of Members

10% of Members



- 40% Share Intel
- 10% In January 2018

- **What I have learned about ISACs and Information Sharin**g
    - A clear mission matters
    - TRUST is the foundation of Intelligence and Information Sharing
    - A integrated technical platform for intel sharing & analysis is fundamental
    - The Role of the Cyber Threat Intelligence Analyst is only beginning.

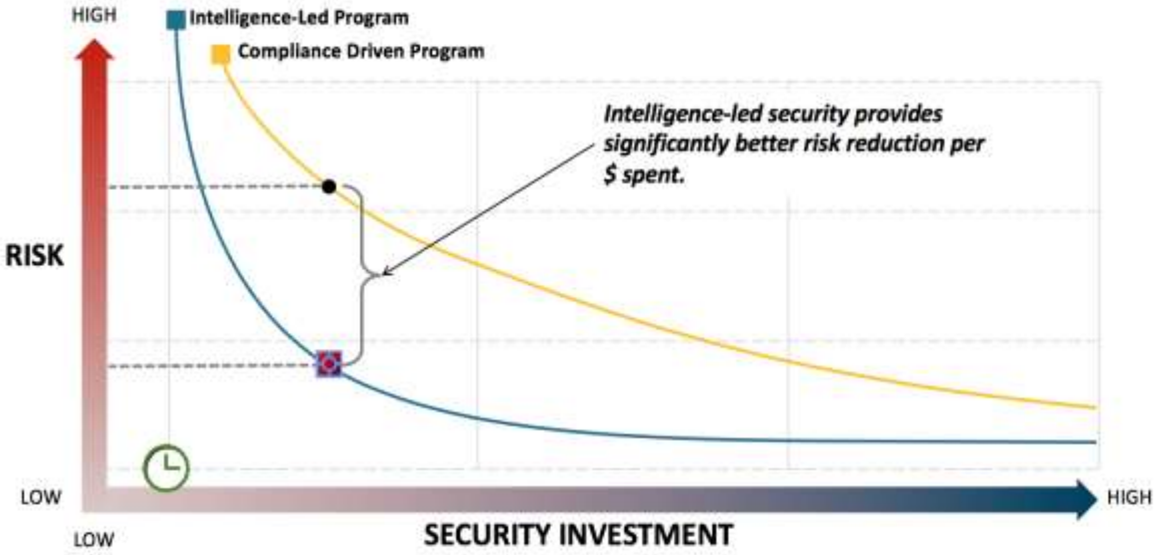
“Cyber threat intelligence is knowledge about adversaries and their motivations, intentions, and methods that are collected, analyzed, and disseminated in ways that help security and business staff protect critical assets of the enterprise.“

- Adversary based
- Risk focused
- Process oriented
- Tailored for diverse consumers

SOC analysts may want just enough context to escalating to the IR team.

IR may want very detailed context to determine if an alert is related to other events on the network.

CISO may want to align with business risk and critical assets.



Industry Needs

1. Industry Threat Intel Sharing
   - Postmortem Breach Analysis is important but NOT sufficient
   - Support for a Proactive & Requirements driven Threat Intelligence Exchange.
   - Government – Industry Partnership

2. CTI Education and Training
   - Education vs technical skill
   - Instructional Systems Design
   - Learning model design

Questions?

Tommy.McDowell@r-cisc.org

INTEL471

ACTOR-CENTRIC CYBER THREAT INTELLIGENCE

Aug. 23, 2018

TLP:AMBER

CVE WEAPONIZATION REPOR

CVE	Type	Report Status	Intel 471 Risk Level*	Patch Status	Interest Level	Location(s) of Activity or Discussion	Exploit Status
CVE-2018-11776	RCE	New	High	🟢	🟢🟡	🟢🟡	🐞
CVE-2018-5390	DoS	New	Low	🟡	🟢🟡	🟢🟡	🟢
CVE-2018-0792	RCE	New	High	🟢	🟢🟡🔴	🟢🟡	🚀
CVE-2018-0851	RCE	New	High	🟢	🟢🟡🔴	🟢🟡	🚀
CVE-2017-15429	Info disclosure/code exec.	New	Medium	🟢	🟢🟡🔴	🟢🟡	🟢
CVE-2018-0587	Unrestricted file upload	New	Medium	🟢	🟢🟡🔴	🟢🟡	🟢
CVE-2017-11882	RCE	New	High	🟢	🟢🟡🔴	🟢🟡	🐞 🚀 🛒

* Intel 471 assesses vulnerabilities using a weighted calculation across the following criteria (in descending order of criticality):

- Mitigation status;
- Exploit status; and
- Underground activity.

🟢 Patch available	🟢 Disclosed publicly	🟢 Open source	🟢 Not observed
🟡 Some available	🟡 Researched publicly	🟡 Underground	🐞 Code available
🔴 Patch unavailable	🔴 Exploit sought in underground	🔴 Private communications	🚀 Weaponized
			🛒 Productized

Details

CVE-2018-11776	Status:	**New**	CVSSv3:	**9.8**	Risk level:	**High**	Patch:	**Available**
	Type:	**RCE**	PoC:	**Observed**	Underground:	**Observed**	Detection:	**Unavailable**

CVE summary

CVE-2018-11776 is a remote code execution (RCE) vulnerability impacting multiple versions of the Apache Struts application. The impacted vendor released patching and mitigation information for impacted products and corresponding versions. A proof of concept (PoC) was observed publicly and in the underground.

Underground activity

Intel 471 did not observe weaponization or productization of CVE-2018-11776 in the underground. Intel 471 observed the actor **CyberWarring** advertise an open source article authored by Man Yue Mo; and the actor **pixel1** share a Github page containing PoC details.[1]

CVE-2018-5390	Status:	**New**	CVSSv3:	**NA**	Risk level:	**Low**	Patch:	**Some available**
	Type:	**Denial of service**	PoC:	**Not observed**	Underground:	**Observed**	Detection:	**Unavailable**

CVE summary

CVE-2018-5390 is a denial-of-service (DoS) vulnerability impacting the Linux kernel versions 4.9+. Some of the impacted vendors released patches and/or mitigations. A PoC was not observed publicly or in the underground.

Underground activity

Intel 471 did not observe weaponization or productization of CVE-2018-5390 in the underground. Intel 471 observed the actors **el_cesar** and **MR_smoker** share open source reporting about the vulnerability.[2] [3]

INTEL471

MALWARE INTELLIGENCE

Data Sheet

KEY POINTS

- Automatically operationalize high confidence and timely IOCs with context within your environment
- Reduce the number of incidents you are responding to by blocking IOCs before incidents happen
- Gain insight and understanding of the latest crimeware campaigns
- Access and consume through an online portal, RESTful API and 3rd party integrations
- Supports malware detection, incident response, threat hunting and intelligence use cases
- Everything mapped to MITRE's ATT&CK framework
- Malware intelligence reports
- IDS signatures and YARA rules
- TTP information
- Malware and botnet configuration information including web injects
- File and network based indicators

Moving to an intelligence-led security strategy

Financially motivated cybercriminals are continuously launching new attacks against your organization, sector and customers. Without high confidence, timely indicators with rich context and TTP information, organizations are unable to move from a reactive incident driven security posture to an intelligence lead security strategy.

Coverage and ability to operationalize within your organization

When it comes to malware and technical intelligence, it's all about coverage and how quickly you can operationalize it within your organization. Where was the data and information collected from? How fresh is it? Is it still being used by cybercriminals? When can I expire it from my environment? How do I automatically block badness?

Intel 471's Malware Intelligence offering leverages Intel 471's industry leading access in the cybercriminal underground to obtain early access to malware including trojans, RATs and stealers. This early access allows us to analyze and reverse engineer obtained malware to create signatures (IDS signatures and YARA rules), malware intelligence reports and criminal infrastructure monitoring. As soon as the observed malware families are observed in the wild, we will make you and your security systems aware of it for blocking and detection.

Future malware family support within Intel 471's Malware Intelligence product will be driven by customer feedback.

Benefits of the offering

Seamless and automatically ingested into your security tooling and infrastructure including Threat Intelligence Platforms (TIPs) and Splunk.

Near real-time visibility into the latest cybercriminal malware campaigns in the wild and the latest malware advertised and released by cybercriminals in the underground.

Block and detect malware faster, thereby reducing incidents.

Rich context into everything provided including associated malware family, version, malware intelligence reports, botnet configuration (including parsed web injects), linked indicators, IDS signatures, YARA rules and MITRE ATT&CK framework mapping.