CYBER THREAT INTELLIGENCE (CTI) - CYBER DEFENSE FEED

As a CTI professional, you know that information about cyber security threats that are external to your organization is critical.

You also know that for this information to be intelligence it must be:

- Relevant: must relate to the target enterprise, industry, network and/or assets.
- Actionable: specific enough to prompt a response, change or decision to act or not.
- Valuable: must lead to beneficial business outcomes.

CSIS is a leading provider of actionable and intelligence-driven detection and response services. A core part of our offering is CTI itself and we have a number of high-quality feeds to support organizations with Threat Intelligence Platforms and Teams.

1. CTI is our lifeblood

CTI is at the heart of our company.

This means we leverage synergy effects from incident response cases including proprietary tools like CIRK and Chronos, our MDR service and PhishDB, our anti-phishing solution.

Our dedicated CTI research team has unique insights into malicious infrastructures and is capable of both advanced reverse engineering and tracking threat actor behavior.

For more than a decade, CSIS has been involved with threat actor research and malware targeting the financial sector, which is deployed by the top of the food chain among IT-criminal groups. These groups typically also facilitate access to compromised networks on behalf of other less capable actors in what is known as Crime-as-a-Service.

The data collected from these sources is further correlated with OSINT, passive DNS monitoring and collaboration with external partners to widen the scope and provide even more context.

2. Customers leverage our Feeds to address mission-critical needs

Use case – detection and incident prevention

Feeds with the usage designation Monitor (M), Detect (D) and/or Block (B) are suited to be consumed by any solution in place, which help protect an IT-environment from the threat categories mentioned above. The main purpose would be to detect network traffic attempting to reach a domain or IP-address identified via the feed and either automatically block communication or alert security personnel to closely monitor any associated activity. Outgoing traffic would suggest a possible infected host inside the network, whereas incoming traffic could be threat actors scanning the perimeter looking for vulnerabilities or manually trying to compromise the network.

Use case – investigation, containment, and postmortem (incident response)

Unfortunately, it is not always possible to prevent a security incidence even with the best security solutions and personnel. However, if threat actors successfully compromised a network, CSIS feeds are quickly updated and can help in the following incident response investigation. It can also be cases where e.g., IP-addresses are not blocked because they can also host legitimate services necessary for business operation. The feeds with the usage designation Incident Response (IR) are suited for helping shed some light on what happened by e.g., comparing the time stamps of suspicious activity with IOCs from the CSIS feed including the checksum/hashes of known malicious files.

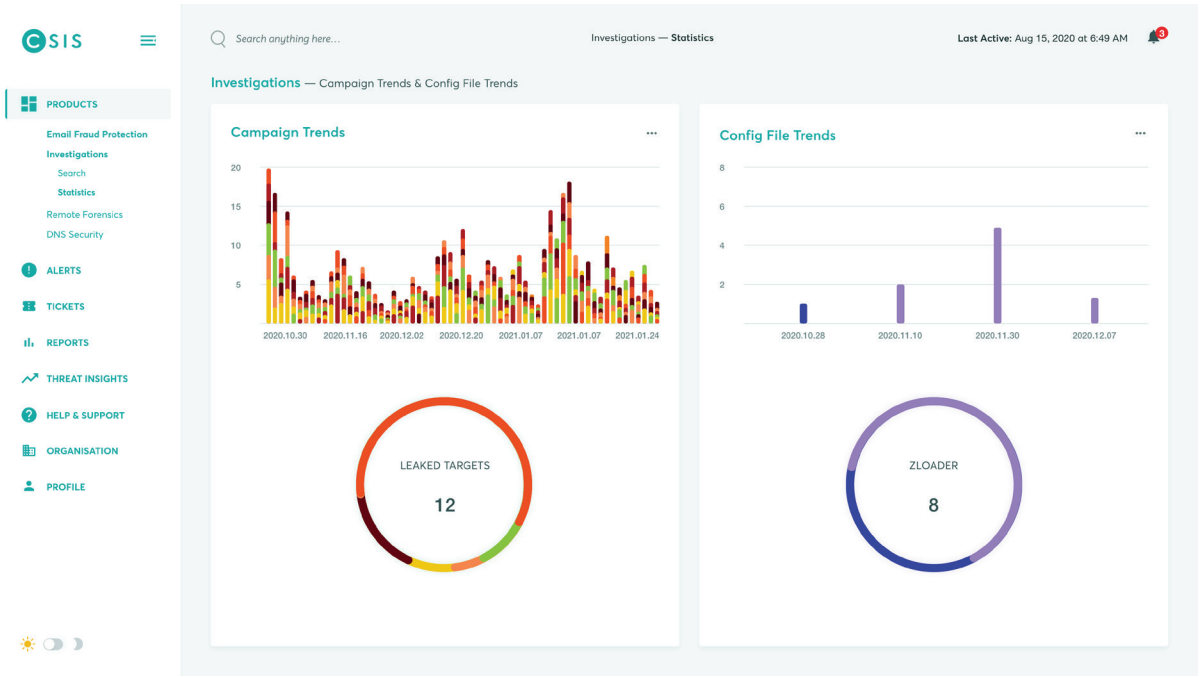
Use case – research and data enrichment

In large or specialized organizations with in-house security research capabilities, the CSIS feeds with the usage designation Research (R) and Enrichment (E) are valuable to complement on-going investigations of a particular malicious campaign or threat actor activity as well as enrich data collected elsewhere to get a more complete picture of the scale, purpose, and severity. For example, CSIS is tracking eCommerce sites compromised by form-jacking Java Scripts (a.k.a. Magecart attacks). This information can be correlated with both network traffic and fraudulent activity implicating credit card customers of financial service providers.

Use case – Early Warning

Financial and critical infrastructure organizations or businesses with extended supply chains can all benefit from the feeds with the usage designation Early Warning (EW). These can warn about changes in the target list of malware configuration files suggesting imminent attacks, data leakage related to a supply chain partner because of a ransomware attack or information about a threat actor e.g., involved in phishing activity in geographical areas or against targets of particular interest or concern.

Investigation - Campaign Trends & Config File Trends



3. We have 9 high-quality feeds

Feeds	Description	Usage designation*						
		M	D	B	IR	R	E	EW
Full Crimeware	Full access to the CSIS crimeware database covering information related to malicious online activity.	●	●	●	●	●	●	●
Malware Campaigns (IOCs)	List of IOCs and IOAs.	●	●	●	●	●	●	
Malicious Domains (DNS)	List of malicious domains controlled or compromised by threat actors.	●	●	●	●	●	●	
Malware Infected IPs	List of infected IPs related to malicious infrastructure.	●	●		●	●	●	
Possible Remote Proxy (PRP)	Feed of IPs likely to be used as a proxy for IT-criminals.	●	●		●	●	●	
Malware Configuration Files	Decrypted trojan configuration files revealing the targets of the malware.	●				●	●	●
Leaked Targets	Feed of companies compromised by ransomware, which led to data leakage on the Internet.	●				●	●	●
Threat Actor Intelligence	Feed of Threat Actor MO (modus operandi), toolset, origin, domain registration details, online profiles, and aliases.	●	●	●	●	●	●	
Phishing (Kits and URLs)	Feed of URLs and phishing kit source code.	●	●	●	●	●	●	

**Usage designation: Monitor (M), Detect (D), Block (B), Incident Response/handling (IR), Research (R), Enrichment (E), Early Warning (EW).*

4. Malware IOC Categories

The Malware Campaign feed includes all indicators related to a particular type of threat. CSIS currently operates with the following main categories:

APT	Primarily covers state-sponsored groups targeting governments and critical infrastructure.
Adware	Less intrusive malware primarily focused on changing browser settings, search engine manipulation, and pop-up advertising.
Banking Trojans	Sophisticated malware with a broad specter of capabilities including complete takeover of the infected host, Man-in-the-Middle, Man-in-the-Browser, persistence, harvesting of credentials and contacts from mail clients, brute forcing of passwords, lateral spreading, and network reconnaissance.
Botnets	Widespread infections also involving IoT devices used for e.g., proxy activity, spam, and DNS manipulation.
DDoS	Confirmed infections abused in DDoS activity.
Exploit Kits	Malware used on websites to infect visitors by exploiting vulnerabilities in browsers.
InfoStealer	Malware designed to steal sensitive information including logon credentials, documents, and contact lists.
IoT	Internet of things malware primarily infecting e.g., routers and surveillance cameras.

Loader	Malware responsible for downloading additional payloads – often seen as first step before a more serious infection of e.g., banking trojans.
Mobile malware	Malware dedicated mobile platforms, which means primarily Android.
Phishing	URLs hosting phishing kits used for impersonating well-known brands to compromise logon credentials for financial services or e-mail accounts.
PoS	Point of Sales malware used to infect PoS networks in order to compromise credit card information.
RAT	Remote Access Tools acting as backdoors giving threat actors complete control of the infected device – also exist as legitimate software used for remote support by IT-departments.
Ransomware	Highly destructive malware usually following infections by Loaders and/or banking trojans leading to complete infrastructure encryption if not mitigated.
Rootkit	Persistent malware capable of surviving OS reinstallation by infecting the BIOS/UEFI sector.
Sinkhole	Malicious domains taken over the security industry to protect infected hosts.
Threat Actors	Intelligence about specific threat actor individuals and groups.

5. Access and Integrations

All of our feeds can be consumed directly via an API.

Our Malware Campaign Feed also support integrations with:

ANOMALI

KING & UNION

ThreatMetrix
A LexisNexis® Risk Solutions Company

Additionally, the following feeds support Maltego:

Malware Campaign
Malicious Domains
Malware-Infected IPs
Possible Remote Proxy
Malware Configuration Files
Leaked Targets

MALTEGO

REST ASSURED.

CSIS IN BRIEF

- Founded in 2003
- Leading pure-play cybersecurity services player
- Delivering actionable and intelligence-driven detection and response services
- Preferred partner to leading organizations across multiple sectors
- Trusted advisor to law enforcement agencies, government and news media
- Credited by Gartner

OUR OFFERING

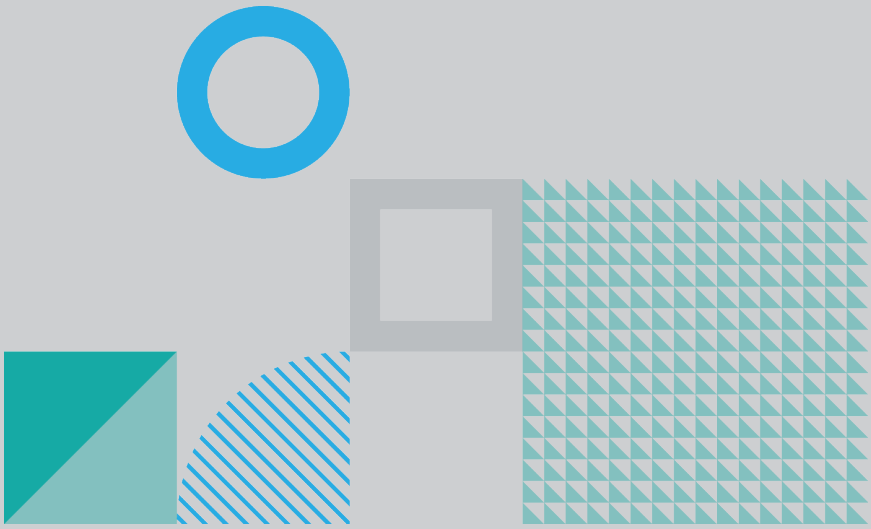
- Managed Detection & Response (MDR)
- Cyber Threat Intelligence (CTI)
- Brand Protection
- Emergency Response Consulting
- Security Consulting
- Security Software

CSIS Security Group A/S

Head office
Vestergade 2B, 4th floor
1456 Copenhagen
Denmark

UK office
95 Aldwych
London, WC2B 4JF
UK

+45 88 13 60 30



www.csis.com