BOTNET INTELLIGENCE

Gain real-time visibility into cybercriminal trends

Since the early 2010s, botnets have become the most popular and lucrative attack tool of cybercriminals. Botnets have targeted critical infrastructure in every sector,led by enterprising cybercriminals who constantly research new vulnerabilities and technical exploits.

The abundance of Malware-As-A-Service ("MaaS") technology brings a new dimension to the severe threat botnets pose. Criminal botnets can support and deliver a broader range of malware variants than ever before, threatening critical infrastructure in new ways.

Botnets and MaaS campaigns have been an R&D priority for PRODAFT since launching the U.S.T.A. platform in 2012. Today, organizations can benefit from that research, using the platform to effectively protect their personnel, customers, and affiliates against MaaS-supported botnet attacks.

Superior Detection of Command and Control Servers (C2s)

PRODAFT's ability to quickly and reliably detect Command and Control servers is a fundamental resource for U.S.T.A. threat intelligence capabilities. The platform allows users to identify these servers on both clear and dark web networks.

PRODAFT has detected and taken down ***more than 59'691 Command and Control servers*** as of 2021 and is constantly searching for new ones.

By collecting URL and IP data from these servers and mapping their features on a mass scale, PRODAFT achieves three essential security goals. The team analyzes this data to:

- Scan organizations' infrastructure and networks for signs of early infection using U.S.T.A. ThreatStream API feeds;
- Investigate ongoing MaaS trends and prepare for the threat landscape of the near future using the Malware Analysis Report Notifications on the U.ST.A. platform;
- Identify the newest techniques and tactics of organized cybercrime groups, find out how they select victims, extract data, bypass existing security technologies,and publish that insight in the U.S.T.A. Tactical Intelligence reports.

COMPROMISED CORPORATE CREDENTIALS

Monitor privileged accounts to mitigate external risks

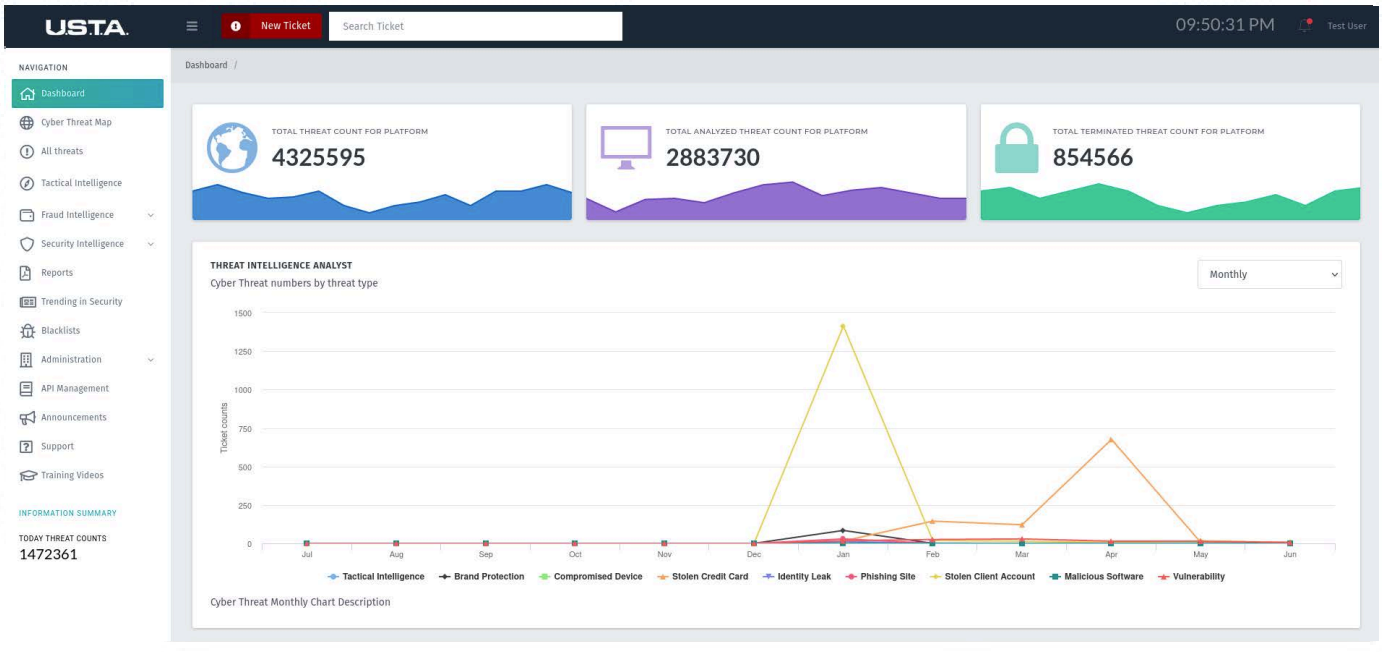
PRODAFT

According to U.S.T.A. metrics, the average mid-sized enterprise (>5'000 users) experiences between ***100 and 300 compromised credentials each year***. Compromised accounts present a fundamental threat to information security because privileged users can often bypass security policies.

U.S.T.A.

U.S.T.A. has analyzed more than 50'000 Command and Control servers, filtering through more than ***5 million credentials every year.*** U.S.T.A. notifies member organizations when cybercriminals use MaaS campaigns to steal corporate credentials.

The platform's Compromised Corporate Credentials section shows relevant alerts for these findings. Users can feed this data into their EDR/XDR solution using the U.S.T.A. ThreatStream API infrastructure.



Threat Intelligence Monitoring, U.S.T.A

Cybercriminals typically use these credentials as an initial entry point for an organized ransomware attack. Detecting compromised credentials is extremely important for external risk mitigation.

COMPROMISED CUSTOMER CREDENTIALS

Break the cybercriminal payment chain

U.S.T.A. uses proprietary techniques and technologies to detect corporate credentials that MaaS campaigns have compromised. The U.S.T.A. platform provides information about other types of credential compromise in separate sections, allowing users to assess the priority and criticality of individual alerts.

- Banking institutions, payment processors, e-commerce vendors, and cryptocurrency exchanges face severe losses and reputation damage when cybercriminals target their users with Malware-as-a-Service campaigns.
- U.S.T.A. metrics show that more than 5 million people have become victims of these campaigns.
- U.S.T.A. closely monitors newly emerging botnets, enabling member organizations to act before cybercriminals, protecting customer accounts against loss.

The Compromised Customer Credentials feature allows U.S.T.A. platform members to receive instant notifications when MaaS operations target their customers.

Users may also feed threat alerts directly into their fraud management systems using the ThreatStream API framework. This enables rapid response to emerging credential threats and keeps customer accounts safe.

Since 2012, PRODAFT has offered customized and proactive defense against constantly evolving cyber-attack techniques. Our cyber threat intelligence platform, U.S.T.A., is a key solution for various critical sectors, including banking and finance, e-commerce, fintech, aviation, insurance, IoT, defense, and telecommunication. Thanks to our unique synergy of tactical intelligence, fraud intelligence, brand protection and security intelligence, we provide actionable, proactive and to-the-point intelligence feeds to prevent threats before they evolve into harmful cyberattack incidents.