DarkOwl Response to White House Executive Order on Improving the Nation’s Cybersecurity
Denver, CO - May, 2021

KEY POINTS

- Cybersecurity researchers consistently observe vulnerabilities and incident predictive events appear across underground hidden networks, to which DarkOwl has unique access.
- Threat actors are actively pursuing methods to bypass multi-factor authentication.
- We have intimate knowledge of darknet threat actor conversations, their evolving techniques, and tools on offer across the darknets for exploiting cloud-based computing and hosting architectures.
- Ransomware gangs heavily rely on the Tor network for command and control of their ransomware operations, recruitment of affiliates and communication with victims and the media.
- DarkOwl can assist in due diligence on evaluating historical cyber incidents as documents indexed from the darknet meet legal admissibility requirements.
- By monitoring the darknet for indicators of compromise and discussions about such vulnerabilities, the Federal Government and its agents can have more visibility into predictive threat actor TTPs, including disruptions to supply chains.

DarkOwl is committed to providing the most comprehensive database of darknet and deep web intelligence and reassert its unwavering cooperation to the protection of the nation’s digital infrastructure as highlighted by the White House’s Executive Order (WH EO) on Improving the Nation’s Cybersecurity, dated May 12th, 2021.

The WH’s EO states that the private sector must **“adapt to the continuously changing threat environment”** – an environment where darknet threat data is increasingly critical. Since 2015, DarkOwl has been a technological pioneer in enabling insight into advanced criminal cyber activity in underground digital communities.

ABOUT THE DARKNET

The darknet and deep web are hidden layers of the Internet accessible only through secure authentication or anonymous network protocols. Threat data from across such networks are a critical piece the national cybersecurity intelligence puzzle. The technology DarkOwl leverages to scrape and index anonymous and hidden digital undergrounds are key to the mission of obtaining proactive situational awareness for protection of the nation’s digital infrastructure.

END-POINT DETECTION & RESPONSE (EDR)

The WH EO emphasized the need for **cyber threat hunting and end-point detection and response** in order more efficiently detect vulnerabilities and incidents on government and vendor networks. Our analysts consistently observe vulnerabilities and incident predictive events across underground hidden networks. DarkOwl supports EDR vendors by enabling them to monitor the darknet for mentions of their products or technical applications, and any associated vulnerabilities that would allow threat actors to gain unauthorized network access.

ABOUT DARKOWL

DarkOwl uses machine learning to automatically, continuously, and anonymously collect, index and rank darknet, deep web, and high-risk surface net data that allows for simplicity in searching.

Our platform collects and stores data in near real-time, allowing darknet sites that frequently change location and availability, be queried in a safe and secure manner without having to access the darknet itself.

DARKOWL DATA SOURCES

Tor, I2P, ZeroNet, authenticated forums, darknet marketplaces, IRC, high-risk paste sites, encrypted chat services, and open FTP servers.

PRIMARY CONTACT

Alison Halland
Alison.Halland@darkowl.com
720.552.5296

CLOUD / ZERO TRUST

The WH emphasized **implementing a country-wide vendor standard of Zero Trust Architecture** and private sector adoption of cloud based technologies. This requirement places an increased burden for mitigating security risks on cloud infrastructure providers. Last year, DarkOwl and IBM reported on the increasing threat to cloud-based data systems including AWS, Azure, and Google. In the course of this research, DarkOwl concluded that darknet threat actors are actively conducting attacks against cloud-based computing and hosting architectures to gain unauthorized authentication credentials, exploit vulnerabilities, and compromise the integrity of such systems.[1]

SUPPLY-CHAIN SECURITY

The WH EO stated a pressing need to **"implement more rigorous and predictable mechanisms for ensuring that products function securely."** The need for nationwide supply-chain security was made increasingly evident in the wake of the December 2020 SolarWinds/Sunburst incident that compromised over 30,000 networks across the private and public sector. **"Critical software in Supply Chain Security"** can include anything on the company network from corporate email and CRM software, to basic network protection devices.

DarkOwl has noted a concerted shift by threat actors on the darknet to target third-and-fourth party vendors and apps, or to compromise a central or decentralized source of third-party software components to infect the target software indirectly. DarkOwl has also observed darknet actors openly discussing how to exploit critical baseline network vulnerabilities such as Virtual Private Networks (VPNs) and Remote Desktop Protocols (RDPs).

RANSOMWARE

The WH EO was in immediate response to a significant ransomware attack against the critical infrastructure supplier, Colonial Pipeline. DarkSide, the ransomware as a service (RaaS) group credited with executing the attack, are not the only criminal gang attacking U.S. digital infrastructure. Ransomware gangs heavily rely on the Tor network for command and control of their ransomware operations and will often self-host multiple Tor onion services to interact with the press and their victims.

Since January 2021, DarkOwl has observed 52 new ransomware variants, with many using evolving techniques such as double extortion and double encryption, and over *two dozen* RaaS operators similar to DarkSide that are currently active on the darknet.

CREDENTIALS / RISK ASSESSMENTS

The WH EO highlighted the **need for vendors to use multi-factor authentication** to reduce the likelihood of credential exposure, along with persistent government oversight and auditing of vendor software developed and any associated vulnerabilities assessments. We regularly observe evidence of unreported commercial network compromise with credential data being sold on the darknet, with over 5,100,000 documents from criminal data leaks that contain lists of email addresses and credentials. DarkOwl can assist in due diligence on evaluating historical cyber incidents as documents indexed from the darknet meet legal admissibility requirements and provide key insight in determining if service providers or software have experienced a cyber incident.

While multi-factor authentication tools are a step in the right direction, criminals on the darknet are actively pursuing malicious methods to circumvent these measures. In one such case, we observed hackers offering "SS7 Bypass 2FA" as a product on a darknet market, which is an SMS authentication bypass that is available for any phone number on any phone network. Cybercriminals will continue to bypass security measures such as this and then capitalize on their innovativeness by offering them to others for sale.

Furthermore, DarkOwl's data supports readiness of the Office of the Under Secretary of Defense for Acquisition & Sustainment's Cybersecurity Maturity Model Certification (CMMC) – which recently included U.S.-based security monitoring as a critical requirement for vendors.

[1] https://www.darkowl.com/blog-content/darknet-threats-to-cloud-based-platforms-and-applications) with contributions to IBM's Cloud Threat Landscape Report published in Q2 2020: https://dutchitchannel.nl/647787/ibm-security-cloud-threat-landscape-report.pdf.