Terri Clark
Director of Technical Services
Kansas Legislative Office of Information Services
The Dark Web is designed for anonymity:

- Network traffic routed through encrypted relays to endpoints
  - Each relay adds a layer of encryption
- Websites and data are not indexed
  - Undiscoverable by most search engines
  - DuckDuckGo is an anonymous search engine
    - Operates Tor exit relay
    - Searches are anonymous, no search history or filtered search results
  - Most dark web data is mundane emails, social media, etc.
- Websites use .onion addresses and public keys instead of common URLs
- User IP addresses are hidden, appear as IP address of Exit Relay
- Users connect using special software and Tor browser

From the Hacker News, Kumar, 2014
STATE LEGISLATURES AND THE DARK WEB

Who is using the Dark Web?

- People concerned with privacy
- Activists and Whistleblowers
- Citizens in countries practicing censorship
  - Facebook - facebookcorewwwi.onion
- Criminal activity is easier on the dark web
  - Privacy and anonymity
  - Use of cryptocurrency (Bitcoin) to transfer funds

Is the Dark Web the Wild West?

- The dark web is monitored by law enforcement and cyber professionals
  - Sale of illegal drugs, child pornography, etc.
  - Stolen user credentials
  - Stolen credit card, banking, personal information
  - Stolen Social Security numbers
  - Stolen health data
  - Stolen corporate proprietary and financial data
  - References to an organization or employees
  - Planned activist activity against an organization

Understanding the dark web provides state legislators insight into privacy issues. As states consider data privacy, data breach, and cybersecurity legislation it’s important to fully understand how the dark web is used to profit from stolen data and criminal activity. It’s equally important to grasp how important privacy is to some citizens, and the inconveniences that will be tolerated to protect that privacy.
Shawn Loveland
Applied Researcher
Microsoft Security Response Center (MSRC)
THREAT INTELLIGENCE FROM THE DARK WEB

EXTERNAL THREAT INTEL

Shawn Loveland
MSRC | Dark Web | Applied Researcher
External threat Intelligence expands the visibility of the kill chain

Companies are impacted by cyberthreats from a multitude of attackers. Today most companies have a responsive posture, monitoring for known attacks and waiting for attackers to attack.

Dark web intel allows a company to be more proactive defense of these attacks.

- Aiding companies in prioritizing their defenses
- Proactively preventing attacks
- Identifying the unknown threats
Companies need intel across all three levels of forums

Closed forums where bad actors have to be invited into. Location of best intelligence.

Forums in TOR and websites that just need a username and password. Focus of many intel companies.

Open to anybody on the Internet.

Vetted Forums

Dark Web

Dark Markets
Markets (forums) where bad actors conduct business with other bad actors

Open Forums
Defense against an ecosystem

Defenders are combating an industry, not just hackers and malware

Ecosystem includes criminal (black market) and non-criminal (grey market) services
Services are plentiful and inexpensive

- **0days** price range varies from $5,000 to $8M+
- **Load**s (compromised device) average price ranges
  - PC - $531.84/k
  - Mobile - $675.00/k
- **Denial of Service (DOS)** average prices
  - Day: $92.67
  - Week: $330.00
  - Month: $959.17
- **Proxy** services (evade IP geolocation) prices vary
  - As low as $100 per week for 100,000 proxies.
- **Ransomware**: $66 upfront or 30% of the profit (affiliate model)
- **Spearphishing services** range from $100 to $1,000 per successful account take over
- **Bulk compromised accounts** As low as $150 for 400M. Averages $0.97 per 1k.
- **Enterprise compromised accounts** As low as $10,000 for a company’s GAL and 100 compromised corporate accounts
How threat intel is incorporated into Microsoft

Intel collected

- Identifying current threats and future threats with up to a six-month forward-looking horizon
- Monitor the kits and services attackers use
- Monitoring changes in attacker monetization strategies
- Collecting cybercriminal tradecraft
- Monitor intel on vulnerabilities as they through their three phases

Why threat intel from is important

<table>
<thead>
<tr>
<th>Supporting internal Microsoft teams to identify unknown current and future threats</th>
<th>Aides our customers tenants to prioritize their patch management based on what vulnerabilities are or will be attacked (N/0 days)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Used by internal Red teams to create new scenarios</td>
<td>Aid MTE hunters and analysts to stay abreast of new and future threats</td>
</tr>
</tbody>
</table>
Summary

- **What is threat intelligence**
  - Expands a company’s visibility into their kill chain
  - Aids companies in prioritizing their defenses
  - Proactively prevents attacks
  - Identifying the unknown threats

- **Not all threat intelligence is the same**
  - Intel is needed across the level of forums, attacker personas, and regions
  - There are geographic and cultural differences that impact attackers TTPMs

- **Why intel from the dark forums is important**
  - Context to the attacks against
  - Understanding the capabilities of the cybercrime ecosystem
  - Disrupt the predictability of the attacker’s ROI
Luke McNamara
Principal Analyst
FireEye Mandiant Intelligence
DARK WEB INSIGHTS

- Useful for answering questions about overall trends in cyber crime /financially motivated threat activity
- Forum or market focus can vary: carding, database, access, malware/tools, other
- Language capability
- Access:
  - some dark web markets also accessible in clear web
  - Some underground markets are on messenger platforms (Telegram, WhatsApp, and even Facebook)
  - Combination of free to join, requiring small fee, further vetting/invite only
- Less useful for visibility into latest APT/nation state activity and behavior
- Cryptocurrency usage
- Evaluating veracity of postings
Threat actor “G” observed since 2011, appears to specialize in website compromises as they have been observed selling access to various websites, including SQL injections, website databases, and shell accesses to enterprises.

Forum posts demonstrate that the actor's operations have impacted numerous organizations.

We identified a set of intrusion operations “Cluster D” that date to at least July 2018.

We observed this activity set attempt multiple compromises of numerous organizations using the same initial vector toolsets, domains, and infrastructures as “G” described in forum postings.

For example, In late September 2018, “G” started a discussion in a Russian-language underground forum where they asked for advice with an active intrusion. Notably, this timeframe overlaps with multiple intrusions we have attributed to the aforementioned “Cluster D”.

On March 19, 2020, on a popular Russian-language forum, actor "B" advertised a ransomware affiliate program. The actor was seeking a limited number of partners to compromise large networks.

- Actor “B” had joined the forum the day prior.
- The actor stated that targeting of organizations in countries from the Commonwealth of Independent States (CIS) is forbidden.
- Affiliate model:
  - More than $200,000 USD per week – 90/10 profit share
  - $100,000-$200,000 USD per week – 85/15 profit share
  - Less than $100,000 USD per week – 80/20 profit share
- Since May threat activity attributed to this ransomware family has impacted a wide variety of sectors, often leaking victim data publicly in addition to ransomware operations?
Will cyber-crime oriented underground forums (especially those specializing in tools and services like ransomware) face increased risk of prioritization by LE for disruption as ransomware continues to pose a widespread disruptive threat?

Threat actors selling access in underground forums can make one of the most important aspects of threat intelligence—attribution—all the harder....Who is the end user?

Evidence of increasing interest within underground forums of monetizing access to operational technology (OT) networks and assets ...how might this shape the threat landscape?
Questions?

Contact
Kae.Warnock@ncsl.org