DNS Abuse in the Age of CoViD-19

IGF 2020 Pre-Event #47
2 November 2020
Today’s Agenda

1. Introduction to DNS
2. DNS Abuse: What is It and Why?
3. DNS Abuse and CoViD-19: ICANN’s View
4. DNS Abuse and CoViD-19: CTI-League’s View
Today’s Presenters

Elena Plexida
Vice President, Government & IGO Engagement

Adiel Akplogan
Vice President, Technical Engagement

Dr. Samaneh Tajalizadeh khoob
Lead Security, Stability, & Resiliency Specialist

Marc Rogers
Vice President, Cybersecurity at OKTA Co-Founder of the CTI-League
Introduction to DNS
The DNS is a Fundamental Internet Technology

E-mail

The DNS was created to solve an e-mail problem.

Elena.Plexida@icann.org

Everything to the right of the @ sign uses the DNS to resolve.

The World Wide Web

Humans do not easily remember IP addresses

Instead of navigating to 192.0.7.10, it is much easier to navigate to www.icann.org.

And it is a lot easier to remember!

Brands

The domain name is a brand identity, regardless of whether an organization is commercial, governmental, educational, or otherwise.
Most Internet users are not aware of the DNS.

They do not realize they use it 100+ times each day.

In turn, they expect it will always work. If it does not work, they call their ISP and report “The Internet is down!”
Users Expect the DNS Will be Secure

A Secure DNS

- Internet users can navigate to the correct sites
- E-mail is delivered properly to the intended recipient
- Apps can be trusted to do what they are expected to do

An Insecure DNS

- Navigation unexpectedly takes us to the wrong site
- Our computing devices become infected with malware
- Our identities or our money are stolen from us
Introduction to DNS Abuse
Cyber Criminals Target the DNS

The DNS is an invaluable tool for bad actors. It can be targeted to aid criminals in their attacks against sites and on individuals.
DNS Abuse

- Disrupt the DNS and you disrupt merchant transactions, government services, social networks
- Exploit the DNS and you can trick, defraud or deceive users
- Vectors for exploitation:
  - Maliciously register domain names
  - Hijack the process the DNS uses to “resolve” the IP address behind a domain name
    - Cache Poisoning
  - Hijack the registration process or data that underpins the DNS
  - Corrupt the DNS data on devices
    - Malware that changes a device’s resolver ← this is really bad and hard to detect
Users are Generally Unaware of DNS Abuse
Enter the Pandemic

CoViD-19

What happens when you combine the motivation of bad actors to attack the DNS with a global pandemic?
DNS Abuse in the Age of CoViD-19: ICANN’s View
• Big events have associated bursts of domain name registration
• COVID-19 no different
  – The extra related stress, worry and working from home makes it the perfect storm
Domain trends update

(Source: John Conwell, DomainTools)
How Does our Identification Approach Work?

• Our approach for identification:
  – Pandemic-related keyword search within zone files (gTLDs + a few ccTLDs)
How Many Domains Have We Identified?

- 662,111 domains were identified since January 2020
What Keywords do These Domains Contain?

• Most of the domains related to 3 keywords
  – 4 keywords account for 73% of the domains
  – Different keywords categories:
    • Disease name (covid, ncov, sars, …)
    • Pandemic countermeasures (mask, lockdown, quarantine, …)
    • Collateral (zoom, webex, conference, …)
  – Significant number of domains matches non-English terms

<table>
<thead>
<tr>
<th>Language</th>
<th>%Domains</th>
</tr>
</thead>
<tbody>
<tr>
<td>English</td>
<td>94.21%</td>
</tr>
<tr>
<td>German</td>
<td>2.13%</td>
</tr>
<tr>
<td>French</td>
<td>1.26%</td>
</tr>
<tr>
<td>Spanish</td>
<td>0.71%</td>
</tr>
<tr>
<td>Dutch</td>
<td>0.68%</td>
</tr>
<tr>
<td>Turkish</td>
<td>0.59%</td>
</tr>
<tr>
<td>Italian</td>
<td>0.14%</td>
</tr>
<tr>
<td>Hindi</td>
<td>0.11%</td>
</tr>
<tr>
<td>Malay</td>
<td>0.08%</td>
</tr>
<tr>
<td>Japanese</td>
<td>0.04%</td>
</tr>
<tr>
<td>Portuguese</td>
<td>0.02%</td>
</tr>
<tr>
<td>Chinese</td>
<td>0.02%</td>
</tr>
</tbody>
</table>
Interpretation?

This is “data”, not “intelligence”

There will be benign domains, unrelated domains, defensive registrations, parked domains… along with anything malicious

What evidence can we find, do we trust it?
API Calls – VirusTotal

<table>
<thead>
<tr>
<th>DETECTION</th>
<th>DETAILS</th>
<th>RELATIONS</th>
<th>COMMUNITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>AllenVault</td>
<td>Malicious</td>
<td></td>
<td>CyRadar</td>
</tr>
<tr>
<td>Emsisoft</td>
<td>Phishing</td>
<td></td>
<td>ESET</td>
</tr>
<tr>
<td>Fortinet</td>
<td>Phishing</td>
<td></td>
<td>G-Data</td>
</tr>
<tr>
<td>Google Safebrowsing</td>
<td>Phishing</td>
<td></td>
<td>Kaspersky</td>
</tr>
<tr>
<td>Netcraft</td>
<td>Malicious</td>
<td></td>
<td>Sophos AV</td>
</tr>
<tr>
<td>Spamhaus</td>
<td>Phishing</td>
<td></td>
<td>ADMINUSLabs</td>
</tr>
<tr>
<td>AegisLab WebGuard</td>
<td>Clean</td>
<td></td>
<td>Antiy-AVL</td>
</tr>
<tr>
<td>Artists Against 419</td>
<td>Clean</td>
<td></td>
<td>Avira (no cloud)</td>
</tr>
<tr>
<td>BADWARE.INFO</td>
<td>Clean</td>
<td></td>
<td>Baidu-International</td>
</tr>
<tr>
<td>BitDefender</td>
<td>Clean</td>
<td></td>
<td>BlockList</td>
</tr>
</tbody>
</table>
CCTC Top Indicators

Indicators of Compromise (66067)

Types of Indicators

<table>
<thead>
<tr>
<th>TYPE</th>
<th>INDICATOR</th>
<th>TITLE</th>
<th>ADDED</th>
<th>ACTIVE</th>
<th>RELATED PULSES</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain</td>
<td>tempatidurpasien.com</td>
<td></td>
<td>Jun 3, 2020, 2:17:16 PM</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>URL</td>
<td><a href="https://it.com/EggFYyNNAN">https://it.com/EggFYyNNAN</a></td>
<td></td>
<td>Jun 3, 2020, 2:17:16 PM</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://www.meduchet.com/cmi/21138163051d1d6766536c26.71326395install">http://www.meduchet.com/cmi/21138163051d1d6766536c26.71326395install</a>...</td>
<td></td>
<td>Jun 3, 2020, 2:17:16 PM</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>URL</td>
<td><a href="https://secure.runescape.com-un.ru/m=weblogin/foginform193,53,674,81">https://secure.runescape.com-un.ru/m=weblogin/foginform193,53,674,81</a>,...</td>
<td></td>
<td>Jun 3, 2020, 2:17:16 PM</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
API Calls - Phishtank
The site ahead contains malware

Attackers currently on malware.testing.google.test might attempt to install dangerous programs on your computer that steal or delete your information (for example, photos, passwords, messages, and credit cards).

- Automatically report details of possible security incidents to Google. [Privacy policy]

Details

Back to safety
Jan 2020 to Sep 2020
- Detected 235,521 pandemic-related domains (both legit and malicious)
- Only phishing and malware distribution

May 2020 to Sep 2020
- Consistent collection and analysis period
  - Detected 134,332 pandemic-related domains (both legit and malicious)
  - Of these, 8,577 (6.4%) domains had one or more reports in phishing/malware reputation lists and had nameservers or resolved to an IP address
  - High confidence reports: 2,329 (1.7%) domains

- Reporting of high confidence domains to registrars started in June
COVID-19: Our Output

Roughly an order of magnitude lost at each gate:

- Thousands of registrations per day
- Some reports on hundreds
- Sufficient evidence on tens
There is definitely bad stuff out there!

BUT: it is not anywhere near the levels that some figures would suggest
DNS Abuse in the Age of CoViD-19: CTI-League’s View
Most Companies Were Rushed into Pandemic Operations

Yet 25,000+ CVEs (vulnerabilities) reported by September

(Previous record 16,500+ in 2018)
The CTI league

- A globally distributed team, for a globally distributed problem.
- Defending the medical industry is hard.
- >70% of medical facilities in the US are small with no dedicated security resources.
- If large institutions are struggling to keep up with patching what hope do we have with smaller ones?
- Attackers are smart enough to target weaker linked organizations first.

Ohad Zaidenberg, Nate Warfield, and Marc Rogers

Cofounders, CTI League

In March, CTI formed a now 1,500-deep “Justice League” of volunteer hackers to defend the health care sector, and hospitals in particular, from cybercriminals exploiting the Covid crisis.

https://CTI-League.com
CTI-League demographics

- The CTI-League is a cross-industry, volunteer org co-founded by Marc Rogers, VP Cybersecurity at Okta

- 1500+ members cover 80 countries and 22 timezones
  - 10% from GOV/LEO worldwide
  - 6% from national CERT’s
  - 7% medical and health sector
  - 77% Infosec

- CTI League mission: To protect the healthcare sector during the pandemic
More than half of attacks against healthcare organizations originate from US and EU countries.

Origination does not equal attribution.

Many campaigns have complex infrastructure established globally in advance.

Attacks against healthcare organizations are a global problem.

Source: Upcoming CTI League darknet report.
Collaboration
Much of What is Being Found, Exploited is **Old**

**Results:**
Medical Vulnerabilities
Triaged by CTI-League in 1\textsuperscript{st} Month

**Total vulnerabilities detected in one month:** 2,000+
found in high risk medical organizations

**Sample of Vulnerabilities detected in just one week:**

- RCE vulnerability – 22
- BlueKeep vulnerability – 2
- SMBv3 open ports – 2
- Citrix Gateway servers – 21
- Less prioritized CVE vulnerabilities – 5
- Exposed Xero Universal Viewer instances – 3

*Data from CTI-League Report, March 2020*
However, we also need to learn from past mistakes.

- 2020 has seen some of the simplest critical exploits released since 1990.
  - Ex: Same directory traversal methodology resulted in CITRIX, and F5 critical vulnerabilities.
- Worse, many initial assessments have been inaccurate
- Organizations large and small are failing to keep up with volume of patches
Broad Spectrum of Threats with a Broad Spectrum of Goals

Individual Employees
- Account and identity theft
- Internal tool compromise

Partners
- Attackers routinely “work the chain of trust” attacking smaller organizations as a way into larger ones

Infrastructure + Data
- Wide use of infrastructure vulns against medical facilities
- Attackers are after Data, IP and Access
- Stolen data routinely found for sale on darkweb
- Stolen accounts are sold or used to enrich other forms of attacks
- Access to compromised companies sold for bitcoin
Simplest Attacks Are the Most Effective

- Isolation leaves employees vulnerable
- Major vishing and phishing campaigns on-going
- Simple vector: sophisticated execution
People are primary targets in 2020

Cyber Criminals Take Advantage of Increased Telework Through Vishing Campaign

SUMMARY
The Federal Bureau of Investigation (FBI) and Cybersecurity and Infrastructure Security Agency (CISA) are issuing this advisory in response to a voice phishing (vishing) campaign.

The COVID-19 pandemic has resulted in a mass shift to working from home, resulting in increased use of corporate virtual private networks (VPNs) and elimination of in-person verification. In mid-July 2020, cybercriminals started a vishing campaign—gaining access to employee tools at multiple companies with indiscriminate targeting—with the end goal of monetizing the access. Using vished credentials, cybercriminals mined the victim company databases for their customers’ personal information to leverage in other attacks. The monetizing method varied depending on the company but was highly aggressive with a tight timeline between the initial breach and the disruptive cash-out scheme.
Results: Domain Takedowns (March 19 – April 14)

Total Takedowns: 2,833

Takedowns by Country:
- Malicious Internet Domains – 2,818
- United Kingdom Institution Impersonators – 2
- Canada Institution Impersonators – 4
- European Union Institution impersonators – 1
- Denmark Institution impersonators – 1
- Morocco Institution impersonators – 1
- Brazil Institution Impersonators – 1
Final Thoughts

Don’t let siloes remain a major challenge:
Stronger together.

OSINT
Yourself and your organization.
Know what’s out there.

Prioritize patching

2020 is challenge, but we have the tools. We need to use them together: Collaboration
Engage with ICANN

Thank You and Questions
Visit us at icann.org
Email: email@icann.org

@icann
facebook.com/icannorg
youtube.com/icannnews
flickr.com/icann
linkedin/company/icann
slideshare/icannpresentations
soundcloud/icann