Uncovering badness using Passive DNS
Agenda

- What is Passive DNS? Benefits of using passive DNS
- Who should be using Passive DNS?
- Use cases
- Q&A
Passive DNS 101

- Passive DNS Replication - Florian Weimer paper at 17th FIRST.org 2005
- Collecting cache miss traffic using sensors
- DNS transactions into a simple format
Why Passive DNS?

- Everything begins with a DNS query
- DNS is used (legitimate queries)
- DNS is also used for abuse by malware -
  1. Phishing domains
  2. Legitimate domains with scripts/web hosting accounts compromised
  3. Botnets, ransomware - C2C mothership
- Domain names are cheap. 99% domains registered are used for malicious purposes
Mapping of the interconnections

- Doing forward lookups (active) poses a risk - targeted domains
- Correlation of domains, name servers, IP addresses
- What other domains are hosted on the same IP address?
- What other domains are using the same name servers?
- What other domains are having the same MX?
Who should be using Passive DNS?

- Malware researchers
- Security professionals
- Incident Responders
- SOC Analysts
- Law Enforcement
Passive DNS operators

- Spamhaus Technology
- Farsight Security
- RiskIQ
- CIRCL
- VirusTotal
What is going on over at GoDaddy?

Published on February 12, 2020

Simon Forster  Follow

One of our researchers has reported over 5,000 hijacked domains to GoDaddy and there seems to be no end in sight. Another 700 today.
The Current State of Domain Hijacking, and a specific look at the ongoing issues at GoDaddy

2020-04-17 12:04:54 UTC  |  by Spamhaus Team  |  Category: domain, dt, domain-hijack, spamth

Domain hijacking is not a new problem, but it is one that gains strength if it is not countered effectively, and we have seen some disturbing trends in the last 6 months.

Cyber criminals are increasingly relying on legitimate and well established domains in order to carry out their maliciousness on the internet. Because of a recent sharp increase in "Business Email Compromise" (BEC) we are seeing more and more domain hijacking.

- The criminals carrying out this activity are using many weapons in their arsenal to gain access to legitimate domains: phishing, social engineering, exploiting vulnerabilities in DNS management software, and delivering malware that gives them access to the unsuspecting user’s information.
- Once they have gained the access to manipulate the DNS of the targeted domains, they will create new hostnames (domain shadowing) that point to a different IP range that is not associated with the root domain, while keeping the root domain intact. Alternatively, they will change the name servers of the domain to point to a new location.
- After they have changed the DNS, they use the positive and well-established reputation of these domains to carry out large scale spam sending and malware hosting campaigns. These are meant to gather more user credentials, infect systems with malware, or disrupt users and businesses to suit their own needs. Using the positive reputation of the stolen domains allows them to evade spam filters and other protection methods that depend on reputational data.

It would be logical to expect that registrars would be on top of the ever-changing landscape that is allowing criminal elements to exploit their users. However, Spamhaus is not seeing enough proactive and mitigating efforts by the world’s largest registrar, GoDaddy. In February we published an article What is going on at GoDaddy? Two months have passed and we still are seeing a continual issue with legitimate domains registered at GoDaddy being hijacked for nefarious purposes.
Domain Shadowing Attack

- Attackers gain access to credentials of legitimate domain names
- Create subdomains pointing to hosting infrastructure (phishing, malware etc)
Dive in #1- Godaddy Domain shadowing

• Bad actors create pxi.domain.tld CNAME pointing to voxpk.duckdns.org
• voxpk.duckdns.org pointing to 104.250.187.36
• pxi.domain.tld contains scripts (phishing, spam etc)
• AS3223 - VOXILITY, GB
"records": [ 
{
  "id": "2BF14A2CF2DCE6391CCA69CF18FED193",
  "rdata": "34.102.136.188",
  "domain": "incometaxnotice.in",
  "rclass": "IN",
  "rrname": "incometaxnotice.in",
  "rrtype": "A",
  "time_last": 1594172528
},
{
  "id": "671FA3C2A30795D65B5AB3D7063C551D",
  "rdata": "ns06.domaincontrol.com",
  "domain": "incometaxnotice.in",
  "rclass": "IN",
  "rrname": "incometaxnotice.in",
  "rrtype": "NS",
  "time_last": 1594153895
},
{
  "id": "9DC7C87EF72C553D325E1335309866F8",
  "rdata": "ns05.domaincontrol.com",
  "domain": "incometaxnotice.in",
  "rclass": "IN",
  "rrname": "incometaxnotice.in",
  "rrtype": "NS",
  "time_last": 1594153895
},
{
  "id": "B187A96418E25FDCC9053947D17CD3F7",
  "rdata": "voxpk.duckdns.org",
  "domain": "incometaxnotice.in",
  "rclass": "IN",
  "rrname": "pxi.incometaxnotice.in",
  "rrtype": "CNAME",
  "time_last": 1594153895
},
{
  "id": "A94F7402A8908F1923A8C95CCA124B4D5",
  "rdata": "ns05.domaincontrol.com. dns.jomax.net. 0 28800 7200 604800 600",
  "domain": "incometaxnotice.in",
  "rclass": "IN",
  "rrname": "incometaxnotice.in",
  "rrtype": "SOA",
  "time_last": 1594172528
}
]}

{
  "id": "B1B7A96418E25FDCC9053947D17CD3F7",
  "rdata": "voxpk.duckdns.org",
  "domain": "incometaxnotice.in",
  "rclass": "IN",
  "rrname": "pxi.incometaxnotice.in",
  "rrtype": "CNAME",
  "time_last": 1594153895
},
<table>
<thead>
<tr>
<th>Name</th>
<th>Last modified</th>
<th>Size</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>csi-bin/</td>
<td>2020-07-09 19:30</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>test.php</td>
<td>2020-06-29 06:13</td>
<td>670</td>
<td>-</td>
</tr>
</tbody>
</table>
Upload is WORKING
Check Mailing...

<table>
<thead>
<tr>
<th>E-Mail</th>
<th>Order ID</th>
</tr>
</thead>
</table>

Send test >>
Welcome to MyDHL

DHL Express is the leader in global express shipping. With MyDHL we offer you an easy-to-use online shipping, tracking and billing solution — customized for your needs.

Learn About the Benefits of MyDHL and Register Now

- Fast and Easy Online Shipping
- Easy Tracking
- One Login for Everything
- Manage your Profile
- Secure and Convenient Access

MyDHL makes it easier than ever for you to track your package.
Dive in #2
"records": [
{
"id": "27D7491C032B652595C18B40F04443A9",
"rdata": "ns-cloud-c1.googledomains.com",
"domain": "netbanksecure.app",
"rclass": "IN",
"rrname": "netbanksecure.app",
"rrtype": "NS",
"time_last": 1594429924
},
{
"id": "E8F7E6196B80BA2FBB7D50DB0BA852C4866",
"rdata": "ns-cloud-c3.googledomains.com",
"domain": "netbanksecure.app",
"rclass": "IN",
"rrname": "netbanksecure.app",
"rrtype": "NS",
"time_last": 1594429924
},
{
"id": "EF6E684C70C30D9926B413AC8FC2DA",
"rdata": "ns-cloud-c4.googledomains.com",
"domain": "netbanksecure.app",
"rclass": "IN",
"rrname": "netbanksecure.app",
"rrtype": "NS",
"time_last": 1594429924
},
{
"id": "FA6C3C3068A0C9BE417953885886827",
"rdata": "ns-cloud-c2.googledomains.com",
"domain": "netbanksecure.app",
"rclass": "IN",
"rrname": "netbanksecure.app",
"rrtype": "NS",
"time_last": 1594429924
}]}
"records": [
{
   "id": "01F82AC93840B30C046FB5770D9DDEDE",
   "rdata": "52.189.217.143",
   "domain": "netbanksecure.app",
   "rclass": "IN",
   "rrname": "netbanksecure.app",
   "rrtype": "A",
   "time_last": 1594429924
}
],
$ dig verifyaccountxvconfirmationvxcenterstxlmmopstui.tk

; <<>> DiG 9.10.6 <<>> verifyaccountxvconfirmationvxcenterstxlmmopstui.tk
; ; global options: +cmd
; ; Got answer:
; ; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 58236
; ; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 5

; ; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; ; QUESTION SECTION:
;verifyaccountxvconfirmationvxcenterstxlmmopstui.tk. IN A

; ; ANSWER SECTION:
verifyaccountxvconfirmationvxcenterstxlmmopstui.tk. 14400 IN A 178.159.36.237

; ; AUTHORITY SECTION:
verifyaccountxvconfirmationvxcenterstxlmmopstui.tk. 299 IN NS ns2.dnsbeonline.ru.
verifyaccountxvconfirmationvxcenterstxlmmopstui.tk. 299 IN NS ns1.dnsbeonline.ru.

; ; ADDITIONAL SECTION:
ns1.dnsbeonline.ru. 14377 IN A 178.159.36.237
ns1.dnsbeonline.ru. 14377 IN A 178.159.36.136
ns2.dnsbeonline.ru. 14377 IN A 178.159.36.89
ns2.dnsbeonline.ru. 14377 IN A 178.159.36.82

; ; Query time: 1369 msec
; ; SERVER: 192.168.0.1#53(192.168.0.1)
; ; WHEN: Tue Sep 08 12:30:48 IST 2020
; ; MSG SIZE  rcvd: 210
FYI, the IP address 8.208.77.188 is hosting many such domains. See attached.
Summary

• Enables investigation of abuse in DNS
• Mapping of the interconnections provides an insight into scale of attack and preparation for takedown
• Passive DNS operator database may not have a full picture
• Passive DNS is a historical database
• Passive DNS - Common Output Format (draft-dulaunoy-dnsop-passive-dns-cof-07)
References

- Passive DNS Replication

- What is going on over at GoDaddy?
  https://www.linkedin.com/pulse/what-going-over-godaddy-simon-forster

- The Current State of Domain Hijacking, and a specific look at the ongoing issues at GoDaddy

- Phish of GoDaddy Employee Jeopardized Escrow.com, Among Others

- Openphish Community Feed
  https://openphish.com/feed.txt

- Spamhaus Technology Passive DNS
  https://www.spamhaustech.com/product/passive-dns/

- Spamhaus Passive DNS API
  https://docs.spamhaustech.com/pdns/docs/source/index.html

- Farsight Security Passive DNS (DNSDB)

- CIRCL Passive DNS
  https://www.circl.lu/services/passive-dns/

- Passive DNS - Common Output Format
Thank you!

• Contact - swapneel@brainattic.in @pswapneel