A Story on DNS Attacks

Once Upon a Time in the West

VALENTINA PALACIN
RUTH ESMERALDA BARBACIL
Threat Library Team

Deloitte Argentina’s Threat Library Team – We gather information about cyber operations being carried across the world to analyze the Motivations, Tools, Tactics and Procedures used by the Advanced Persistent Threats. We aid researchers understand and defend themselves against cyber threats around the globe.
-[ So, what? ]-

Agenda

❖ The Bullets
❖ DNS Attacks 2007-2019
❖ The Gunmen
❖ Guns In Data
❖ Dodging The Bullets

-[ Once Upon a Time In The West ]-
Mitre ATT&CK Framework

Mapping Tools, Tactics, Techniques and Procedures with ATT&CK Framework

«ATT&CK™ for Enterprise is an adversary model and framework for describing the actions an adversary may take to compromise and operate within an enterprise network.»
Recursive Resolver

Where is es.wikipedia.org?

It's at 198.35.26.96

Root Name Server

Where is .org nameserver?

Try 204.74.112.1

TLD Name Server

204.74.112.1

Where is wikipedia.org?

Try 207.142.131.234

SLD Name Server

207.142.131.234

Where is es.wikipedia.org?

It's at 198.35.26.96

- [ Once Upon a Time In The West ] -
DNS Tunneling
Use of DNS as a covert communication channel to bypass a firewall

DNS Hijacking
Manipulation of DNS queries resolutions to redirect users to malicious sites

DNS Poisoning
Corrupted data is introduced into the DNS resolver's cache to make it return a different result

- [ Once Upon a Time In The West ] -
DNS TUNNELING EXAMPLES

- [ Once Upon a Time In The West ] -
DNS HIJACKING EXAMPLE

Figure 1: DNS Hijacking

- [ Once Upon a Time In The West ] -
DNS POISONING EXAMPLE

Figure 2: DNS poisoning

- [ Once Upon a Time In The West ] -
DNS ATTACKS 2007 UNTIL NOW

- [ Once Upon a Time In The West ] -
JULIE AMERO CASE & OPERATION GHOTS CLICK

- [ Once Upon a Time In The West ] -
JUST FOR THE GLORY


- [ Once Upon a Time In The West ] -
Hacktivism & Vandalism

- Universities
- Media
- Social Networks
[-[ DNS Attack History ]-]

By MCA-CRB

Algerian Hacker

S thanks = Mr. Adel & i-hime & Logripoe D2 All Members See

To Be Continued ...

- [ Once Upon a Time In The West ] -
- [ DNS Attack History ] -
BRAZIL HIJACKED

- [ Once Upon a Time In The West ] -
Brazil Hijacked 4,5 million routers affected

- [ Once Upon a Time In The West ] -
THE GREAT CANNON

- [ Once Upon a Time In The West ] -
- [ The Great Firewall ] -

The Great Cannon

2002
Redirected to blocked IP addresses.

2015 - DDoS attacks.
Redirected to legitimate websites *worldwide*.

---

*ThousandEyes – The Ongoing War Between China’s Great Firewall and Circumvention Tools*
- [ Once Upon a Time In The West ] -
- [ Once Upon a Time In The West ] -
Once Upon a Time In The West

PROJECT SAURON
Once Upon a Time

Project Sauron
Suspected
United States
Strategic

ESPIONAGE
Project Sauron

- Real-time status reporting
- T1132 - Data Encoding (Base64 encoding)
- T1005 - Data from Local System
- T1094 - Custom Command and Control Protocol (DNS Tunneling)
Project Sauron

- Custom Command and Control Protocol
- Multilayer Encryption
- Connection Proxy
- Standard Application Layer Protocol
- Standard Non-Application Layer Protocol
- Multiband Communication
- Network Share Discovery
- Remote System Discovery
- System Network Configuration Discovery
- Discovery
- Command and Control
- Persistence
- Lateral Movement
- Execution
- Credential Access
- Collection
- Automated Collection
- Input Capture
- Data from Local System
- Defense Evasion
- File Deletion
- Scripting
- Timing-based Evasion
- Masquerading
- Timestamp
- Exfiltration
- Over Command and Control Channel
- Over Physical Medium
- Over Alternative Protocol
- Third-party software
- LSASS Driver
- Exploitation of Vulnerability
- Third-Party software
- Scripting

---

"Once Upon a Time In The West"

---
Once Upon a Time

DarkHydrus
Suspected Iranian Expert

MILITARY & POLITICAL ADVANTAGE

- [ Once Upon a Time In The West ] -
DarkHydrus – RogueRobin

- T1193 - Spearphishing Attachment
- T1132 - Data Encoding (Base64 encoding)
- T1059 - Command-Line Interface
- T1094 - Custom Command and Control Protocol (DNS A, AAAA, CNAME, TXT, SRV, SOA records)

- [ Once Upon a Time In The West ] -
FINANCIAL HIJACKING

- [ Once Upon a Time In The West ] -
1234567812345678.attacker-domain.com

Point of Sale Hijacked

BernhardPoS & FrameworkPoS
First cases reported

Multigrain and UDPOS
Steal credential card information

- [ DNS Attack History ] -

- [ Once Upon a Time In The West ] -
DNS MESSENGER
a.k.a Powersource

- Public tool
  DNS_TXT_Pwnage

- T1132 - Data Encoding (Base64 encoding)

- T1027 - Obfuscated Files or Information

- T1094 - Custom Command and Control Protocol (DNS A and TXT Records)

- [ Once Upon a Time In The West ] -
Once Upon a Time

OceanLotus
Suspected Vietnamese
Innovator

ESPIONAGE

- [ Once Upon a Time In The West ] -
- [ Once Upon a Time In The West ] -
DNSpionage
Suspected
Iranian
Expert

- [ Once Upon a Time In The West ] -
DNSpionage – Toolset

T1192 - Spearphishing Link

T1132 - Data Encoding (Custom Base 64 alphabet)

T1008 – Fallback Channels

T1094 - Custom Command and Control Protocol (DNS A record)

- [ Once Upon a Time In The West ] -
Global DNS Hijacking

US CERT ALERT

1. DNS REDIRECTOR
2. DNS A RECORDS
3. DNS NS RECORDS

❖ Let’s Encrypt Certificates
Sea Turtle
Unknown
Origin
Strategic

MILITARY & POLITICAL ADVANTAGE

- [ Once Upon a Time in The West ] -
Guns In Data

- [ Once Upon a Time In The West ] -
DNS Hijacking Common Techniques

T110 – BRUTE FORCE
Access to accounts when passwords are unknown or when password hashes are obtained

T1199 – TRUSTED RELATIONSHIP
Adversaries may breach or otherwise leverage organizations who have access to intended victims

T1078 – VALID ACCOUNT
Steal or capture credentials of user or service account earlier in the reconnaissance process
DNS Tunneling Common Techniques

78%  
T1193 – Spear-phishing Attachments
Spear-phishing emails with malicious macro in document relying on user execution

50%  
T1053 – Scheduled Task
WTS to execute programs at system startup or on a scheduled basis for persistence

42%  
T1086 – PowerShell
Executed PowerShell script or used PowerShell to execute commands sent by C2

36%  
T1008 – Fallback Channels
Alternate communication channels if the primary is compromised or inaccessible

- [ Guns In Data ] -

- [ Once Upon a Time In The West ] -
DNS Tunneling

- Preference for A Records
- Base64 encoding
- IP Addressess as binary, hexadecimal or ASCII data

DNS Records Preferences

- A: 50%
- AAAA: 10%
- TXT: 20%
- SRV: 5%
- CNAME: 5%
- SOA: 5%
- Null: 5%
- [ Dodging The Bullets ]-

Let’s Do Better

GENERAL RECOMMENDATIONS

• Monitor Internet Traffic
• Change default configurations in routers
• MFA on domain’s admin portal
• Validate source IPs in OWA/ Exchange logs
• Use access control list for applications
• Unique passwords and password Managers

- [ Once Upon a Time In The West ] -
DNS HIJACKING

• Use Secure DNS
  (DNSSEC, DNSCrypt, DNS Over TLS, DNS Over HTTPS)
• Review your accounts configurations
• Validate A and NS record changes
• Implement Registry Lock
• Review SSL certificates
MONITOR
DNS TUNNELING

- Monitor DNS Traffic and DNS server logs (ELK + BRO IDs)
- Avoid Internal hosts resolution to external domain. Use proxy
- Have a separate set of recursive servers for your mail servers
- Block >512 bytes TCP and UDP >1024 bytes packets
- Block TXT and NULL records*
- Install a IDS/IPS like Snort or Suricata
- Combine dnsmasq and DNS whitelisting policies
THANK YOU!

Valentina Palacín
Ruth Esmeralda Barbacil

- [ Questions & Answers ] -

- [ Once Upon a Time In The West ] -
Bibliography

Schouwenberg, Roel (April 5, 2005). Increasing cases of DNS poisoning being spotted. Available at: https://securelist.com/increasing-cases-of-dns-poisoning-being-spotted/29988/


Lanstein, Alex (February 17, 2009). Bad Actors Part 3 - Internet Path/Cernel. Available at: https://www.fireeye.com/blog/threat-research/2009/02/bad-actors-part-3-internet-pathcernel.html

Golovanov, Sergey (June 3, 2011). TDSS loader now got “legs” Available at: https://securelist.com/tdss-loader-now-got-legs/30844/


Baumgartner, Kurt (March 2, 2012). DNSChanger – Cleaning Up 4 Million Infected Hosts Available at: https://securelist.com/dnschanger-cleaning-up-4-million-infected-hosts-2/32191/

Preuss, Marco (July 6, 2012) The end of DNS-Changer. Available at: https://securelist.com/the-end-of-dns-changer-12/33132/
Bestuzhev, Dmitry (July 10, 2012) Is it the end of the DNSChanger Trojan? Available at: https://securelist.com/is-it-the-end-of-the-dnschanger-trojan-17/33429/


M.Léveillé, Marc-Etienne (May 7, 2013) Linux/Cdorked. A malware: Lighttpd and nginx web servers also affected. Available at: https://www.welivesecurity.com/2013/05/07/linuxcdorked-malware-lighttpd-and-nginx-web-servers-also-affected/

Meyers, Adams (August 30, 2013) DNS – The Lifeblood of your Domain. Available at: https://www.crowdstrike.com/blog/dns-lifeblood-your-domain/
M.Léveillé, Marc-Etienne (February 1, 2014) An In-depth Analysis of Linux/Ebury. Available at: https://www.welivesecurity.com/2014/02/21/an-in-depth-analysis-of-linuxebury/

Vanheuverzwijn, Benjamin (April 1, 2014) Win32/Sality newest component: a router’s primary DNS changer named Win32/RBrute Available at: https://www.welivesecurity.com/2014/04/02/win32sality-newest-component-a-routers-primary-dns-changer-named-win32rbrute/

Ned Moran, Joshua Homan, Mike Scott (August 6, 2014) Available at: https://www.fireeye.com/blog/threat-research/2014/08/operation-poisoned-hurricane.html

Assolini, Fabio (September 2, 2014) Web-based attack targeting home routers, the Brazilian way. Available at: https://securelist.com/web-based-attack-targeting-home-routers-the-brazilian-way/66358/

Martin, Alan (November 1, 2014) Craigslist redirected to prank site via DNS hijack. Available at: https://www.welivesecurity.com/2014/11/25/craigslist-redirected-prank-site-via-dns-hijack/

- [ Once Upon a Time In The West ] -

Lee, Bryan (June 10, 2015) APT Group UPS Targets US Government with Hacking Team Flash Exploit. Available at: https://unit42.paloaltonetworks.com/apt-group-ups-targets-us-government-with-hacking-team-flash-exploit/


Sudeep Singh, Yin Hong Chang (May 22, 2016) Targeted Attacks against Banks in the Middle East. Available: https://www.fireeye.com/blog/threat-research/2016/05/targeted_attacksa.html

Falcone, Robert (May 26, 2016) The OilRig Campaign: Attacks on Saudi Arabian Organizations Deliver Helminth Backdoor. Available at: https://unit42.paloaltonetworks.com/the-oilrig-campaign-attacks-on-saudi-arabian-organizations-deliver-helminth-backdoor/
Guest (Jun 2016) Crouching Tiger, Hidden DNS. Available at: 
https://www.welivesecurity.com/2016/06/02/crouching-tiger-hidden-dns/

Cian Lynch, Dimiter Andonov, Claudiu Teodorescu (June 19, 2016) MULTIGRAIN – Point of Sale Attackers Make an Unhealthy Addition to the Pantry. Available at: 
https://www.fireeye.com/blog/threat-research/2016/04/multigrain_pointo.html

GReAT (August 8, 2016) ProjectSauron: top level cyber-espionage platform covertly extracts encrypted government comms. Available at: https://securelist.com/faq-the-projectsauron-apt/75533/

GReAT (August 9, 2016) THE PROJECTSAURON APT Available at: 

Grunzweig, Josh (October 1, 2016) OilRig Malware Campaign Updates Toolset and Expands Targets. Available at: https://unit42.paloaltonetworks.com/unit42-oilrig-malware-campaign-updates-toolset-and-expands-targets/

- [ Once Upon a Time In The West ] -

Brumaghin, Edmun (March 2, 2017) Covert Channels and Poor Decisions: The Tale of DNSMessenger. Available at: https://blog.talosintelligence.com/2017/03/dnsmessenger.html

Steve Miller, Jordan Nuce, Barry Vengerik (March 7, 2017) FIN7 Spear Phishing Campaign Targets Personnel Involved in SEC Filings. Available at: https://www.fireeye.com/blog/threat-research/2017/03/fn7_spear_phishing.html

Carr, Nick (May 14, 2017) Cyber Espionage is Alive and Well: APT32 and the Threat to Global Corporations. Available at: https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html

Gorelik, Michael (June 9, 2017) FIN7 takes another bite at the restaurant industry. Available at: http://blog.morphisec.com/fn7-attacks-restaurant-industry

Falcone, Robet (July 27, 2017) OilRig Uses ISMDoor Variant; Possibly Linked to Greenbug Threat Group. Available at: https://unit42.paloaltonetworks.com/unit42-oilrig-uses-ismdoor-variant-possibly-linked-greenbug-threat-group/

- [ Once Upon a Time In The West ] -
Falcone, Robert (October 9, 2017) OilRig Group Steps Up Attacks with New Delivery Documents and New Injector Trojan. Available at: https://unit42.paloaltonetworks.com/unit42-oilrig-group-steps-attacks-new-delivery-documents-new-injector-trojan/


Falcone, Robert (November 8, 2017) OilRig Deploys “ALMA Communicator” – DNS Tunneling Trojan. Available at: https://unit42.paloaltonetworks.com/unit42-oilrig-deploys-alma-communicator-dns-tunneling-trojan/

Caspi, Ofer (2019) Mami. Available at: https://macos.checkpoint.com/families/Mami/


- [ Once Upon a Time In The West ] -
The Clyance Team (February 27, 2018) Protect VS Udpso. Available at: https://threatvector.cylance.com/en_us/home/cylance-vs-udpso-malware.html


Lee, Brian (July 25, 2018) OilRig Targets Technology Service Provider and Government Agency with QUADAGENT. Available at: https://unit42.paloaltonetworks.com/unit42-oilrig-targets-technology-service-provider-government-agency-quadagent/
Falcone, Robert and Lee, Brian (July 27, 2018) New Threat Actor Group DarkHydrus Targets Middle East Government Available at: https://unit42.paloaltonetworks.com/unit42-new-threat-actor-group-darkhydrus-targets-middle-east-government/

Wilhoit, Kyle (September 12, 2018) OilRig Uses Updated BONDUPDATER to Target Middle Eastern Government. Available at: https://unit42.paloaltonetworks.com/unit42-oilrig-uses-updated-bondupdater-target-middle-eastern-government/

GReAT (October 1, 2018) Roaming Mantis, part III Available at: https://securelist.com/roaming-mantis-part-3/88071/

Deloitte Interal Sources (October 30, 2018) Canadian Energy company Suncor targeted with "AgentDrable" RAT [Not available for the public]

ESET Research White papers (December, 2018) The Dark Side of The ForSSHE Available at: https://www.welivesecurity.com/wp-content/uploads/2018/12/ESET-The_Dark_Side_of_the_ForSSHe.pdf


Muks Hirani, Sarah Jones, Ben Read (January 9, 2019) Global DNS Hijacking Campaign: DNS Record Manipulation at Scale. Available at: https://www.fireeye.com/blog/threat-research/2019/01/global-dns-hijacking-campaign-dns-record-manipulation-at-scale.html


GReAT (February 13, 2019) DNS Manipulation in Venezuela in regards to the Humanitarian Aid Campaign. Available at: https://securelist.com/dns-manipulation-in-venezuela/89592/
Dumont, Romain (March 1, 2019) Fake or Fake: Keeping up with OceanLotus decoys. Available at: https://www.welivesecurity.com/2019/03/20/fake-or-fake-keeping-up-with-oceanlotus-decoys/


GReAT (April 3, 2019) Roaming Mantis IV. Available at: https://securelist.com/roaming-mantis-part-iv/90332/


Dahan, Assan (May 24, 2017) Operation Cobal Kitty: A Large-Scale APT in Asia Carred Out By the OceanLotus Group. Available at: https://www.cybereason.com/blog/operation-cobalt-kitty-apt

- [ Once Upon a Time In The West ] -
GReAT (April 3, 2019) Roaming Mantis, part IV. Available at: https://securelist.com/roaming-mantis-part-iv/90332/


Counter Threat Research Team (August 27, 2019) LYCEUM Takes Center Stage in Middle East Campaign. Available at: https://www.secureworks.com/blog/lyceum-takes-center-stage-in-middle-east-campaign


Bryant, Matthew (July 09, 2016) The International Incident – Gaining Control of a .int Domain Name With DNS Trickery. Available at: https://thehackerblog.com/the-international-incident-gaining-control-of-a-int-domain-name-with-dns-trickery/

Applied Threat Research Team (July 23, 2019) ABADBABE 8BADF00D: Discovering BADHATCH and a Detailed Look at FIN8’s Tooling. Available at: https://atr-blog.gigamon.com/2019/07/23/abadbabe-8badf00d-discovering-badhatch-and-a-detailed-look-at-fin8s-tooling/