SEPTEMBER 2022

WHITEPAPER

DNS LAYER SECURITY

FROM THE MITRE ATT&CK PERSPECTIVE

DNSSense
Easiest way to be secure

www.dnssense.com

TABLE OF CONTENTS

What is MITRE ATT&CK Framework?

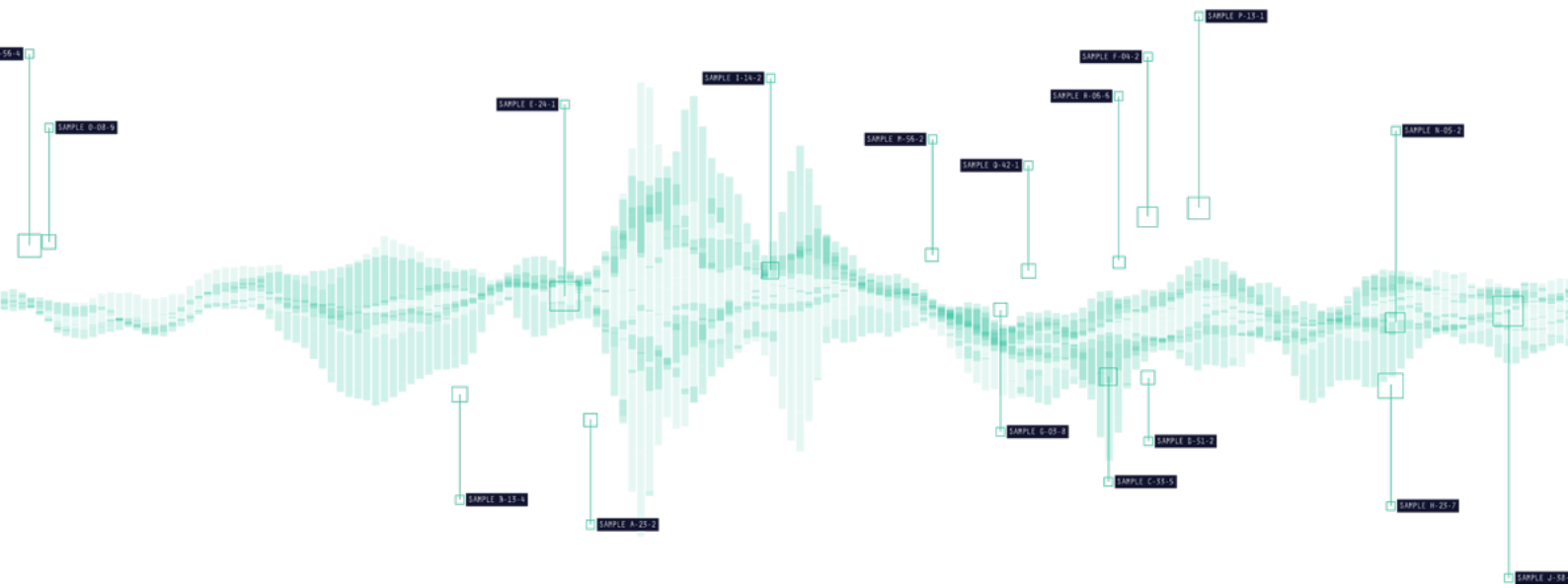
MITRE ATT&CK is one of the most popular methodologies among information security professionals. In the field of information security, MITRE Corporation is known for its CVE (Common Vulnerabilities and Exposures) list cve.mitre.org. This is a database of known vulnerabilities that was launched in 1999 and has since become one of the most important sources for structuring and storing data on software bugs.

Why Do We Need MITRE ATT&CK?

Using data from the MITRE ATT&CK knowledge base, anyone involved in cyber defence can investigate and compare offensive activity and then understand the best options for defence. The framework is a free, accessible, and open knowledge base.

The core of the ATT&CK framework is that it is the most up-to-date information centre showing the behavioural anatomy of an attack and attackers. It was created exclusively by observing cyberattacks in the real world.

MITRE | ATT&CK™



What is ATT&CK?

While collecting and understanding hash values is a broad spectrum, the ATTACK framework helps us interpret this **TTP** (TTP is short for Tactical, technical and procedural).

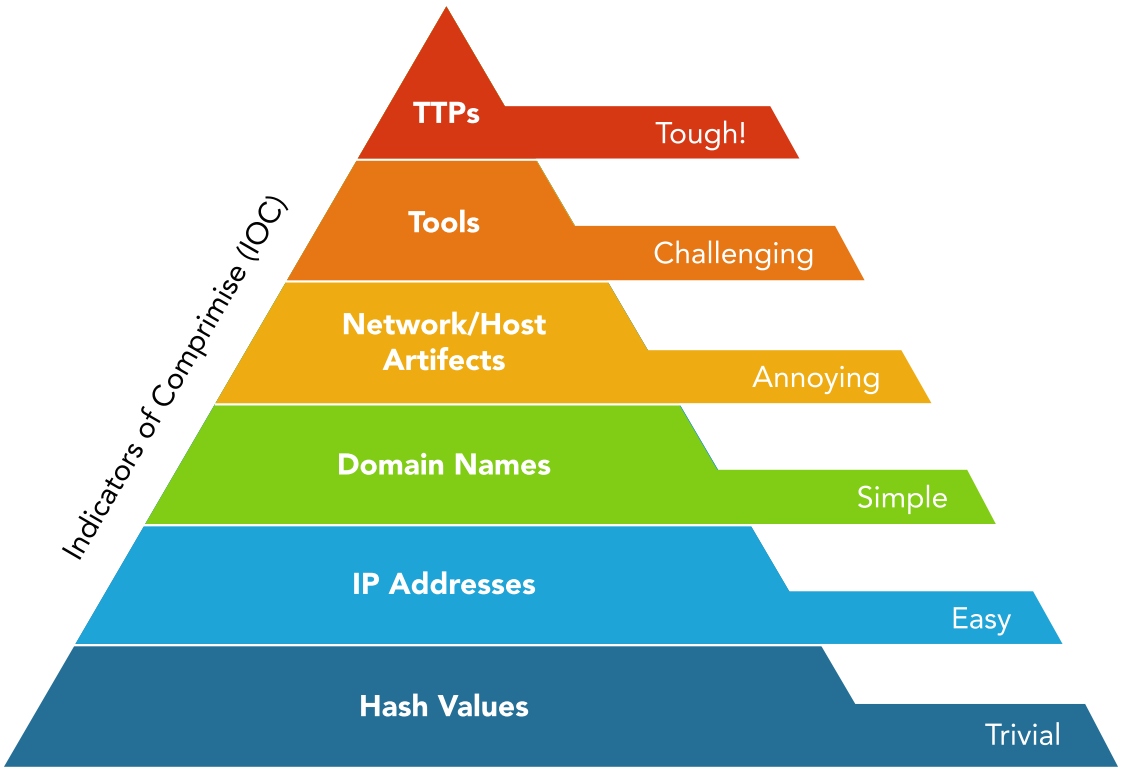
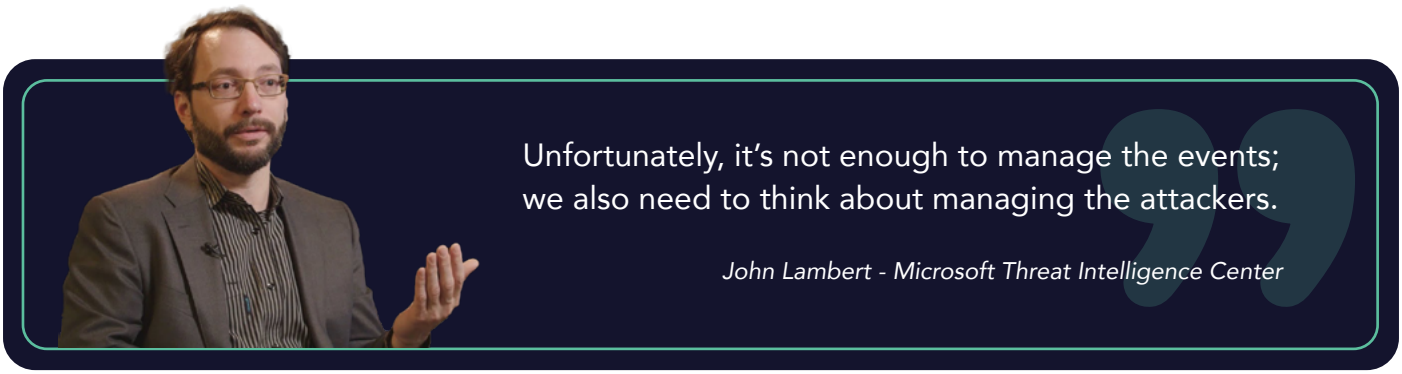


Figure 1 : David Bianco pyramid of pain

IOC (Indicator of Compromise) IOA (Indicator of Attack)

Collecting IOC (Indicator of Compromise) no longer works well in institutions. While IOCs give us piecemeal pieces of a cyberattack that are always static, IOA provides significant Collecting IOCs (Indicator of Compromise) no longer works well in institutions. While IOCs only give us piecemeal pieces of a cyberattack that are always static, IOA offers significant advantages in understanding the attacker's techniques and behavioural analysis to understand the entire attack.



ATT&CK Model

MITRE introduced the ATT&CK matrix in 2013 to describe and categorize aggressor behaviour (behaviour modelling) based on real-world observations. Before we get into the use of the matrix, let us take a look at the basic concepts:

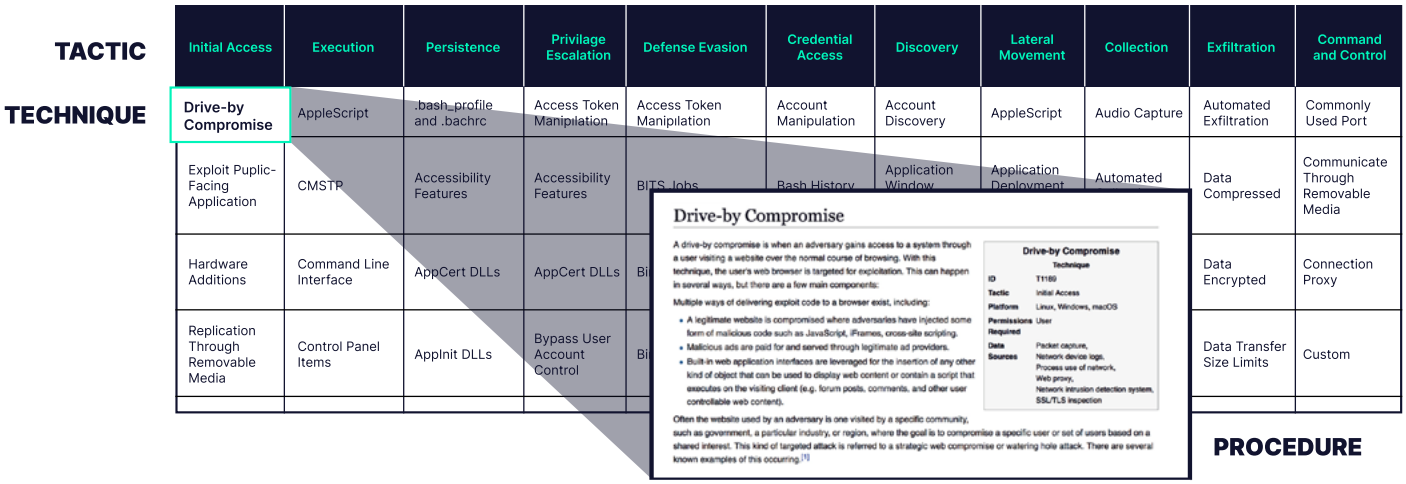


Figure 2 : ATT&CK Model

- **TACTICS**

The way the attacker behaves in the different phases of his operation represents the attacker's goal or the objective he is trying to achieve in a particular step. These are initial access, execution, persistence, privilege escalation, defence evasion, credential access, discovery, lateral movement, collection, command and control, exfiltration, and impact.

Example : TA0002 (The attacker wants to execute malicious code).

- **TECHNICAL**

How the attacker achieved the goal or task, what tools, technologies, codes, exploits, utilities, etc. This is the part where the details are used. Examples of procedures, depending on tactics, are included here.

Example : T1059.001 (PowerShell - using PowerShell in an attack)

- **PROCEDURES**

A set of information showing how and why the technique is used. Procedures include information about attacker groups, descriptions of associated groups, techniques used, version, creation and modification dates, and software.

Example : APT19 (Detailed information on how the technique is executed)

- **MITIGATIONS**

What techniques are addressed by each mitigation method and used to interpret the TTP?

Example : M1056 (Mitigation ID and techniques are in this field)

- **GROUPS**

The method can be read with the group; it is the part where the relationships between the groups and the techniques they use most often are communicated.

Example : G0045 (Identity, other related groups and the techniques they use are here).

- **SOFTWARE**

It is the addressing of malware and tools used by attacker groups.

Example : S0671 (Tomiris tool - Contains information such as type, techniques used, creation and modification dates).

ATT&CK Model - TTP Relationship

The attackers choose their motivation according to tactics as they construct the attack. Again, the relationship diagram above shows which tool and technique or sub-technique must be used to apply the tactic.

MITRE ATT&CK provides an objective environment to assess cybersecurity risks and identify potential vulnerabilities. Once these gaps are known, your organization can make objective decisions about how to address these risks. Your organization can then prioritize and make the best business decisions for deploying security controls and other resources.

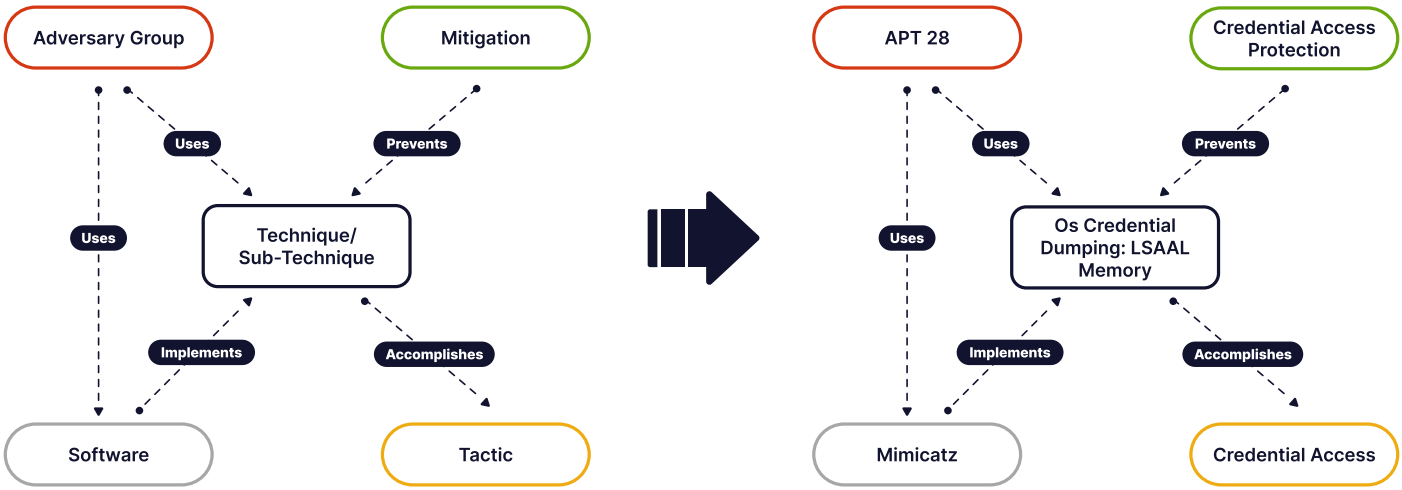


Figure 3 : ATT&CK model – TTP relationship

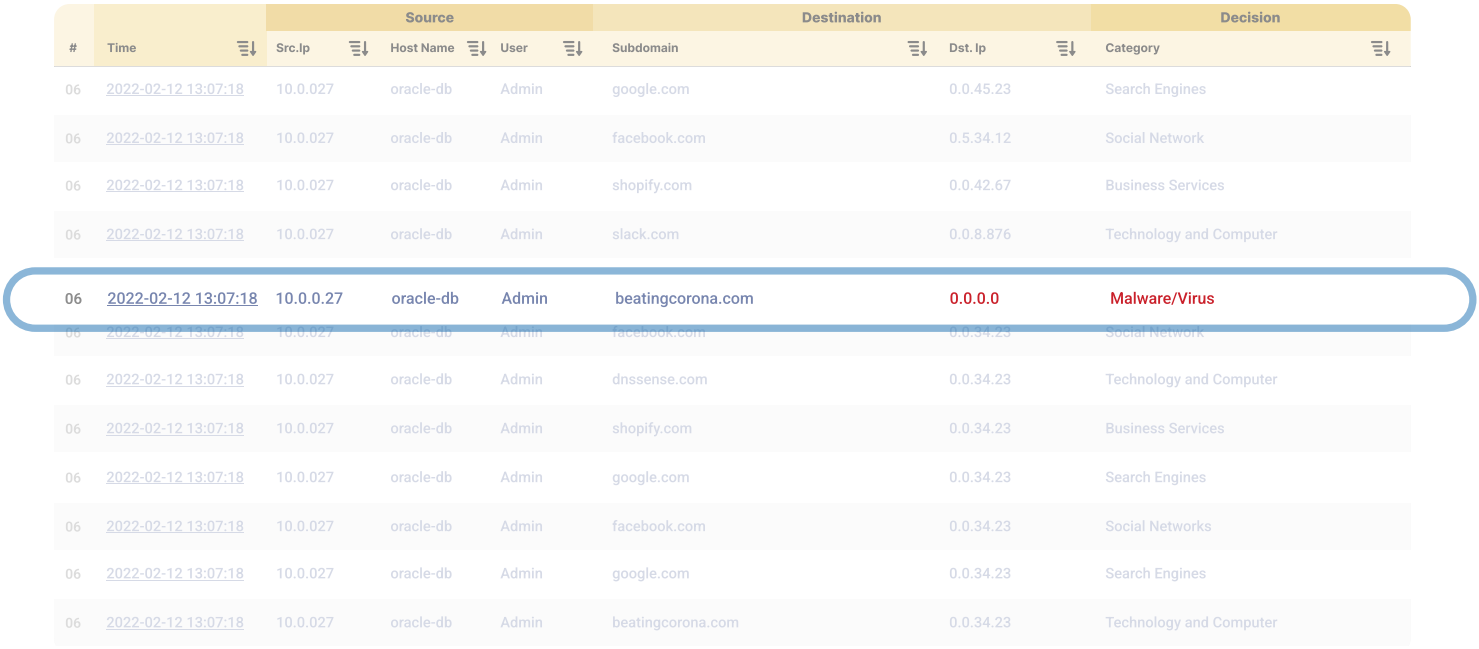
Cyber Kill Chain

Cyber Kill Chain is the attack methodology that determines the sequence of actions that lead the attacker to the target, and Mitre is the ATT&CK methodology library.

Figure 4 : Cyber Kill Chain

In a well-known methodology for cyber attacks, called the cyber kill chain, the steps of a cyber attack are outlined. We know that at least one of these steps must involve a malicious DNS request to trigger an attack.

80% of domains with malware have no immediate IP address, malware requests without an IP address can only be detected in the DNS log. **With DNSSense products, we provide protection and analysis at the DNS level.** It is used by all protocols such as DNS, HTTP, HTTPS, Smtp and IoT. DNS traffic provides information about your entire network, not just the application layer.



		Source			Destination		Decision
#	Time	Src.Ip	Host Name	User	Subdomain	Dst. Ip	Category
06	2022-02-12 13:07:18	10.0.027	oracle-db	Admin	google.com	0.0.45.23	Search Engines
06	2022-02-12 13:07:18	10.0.027	oracle-db	Admin	facebook.com	0.5.34.12	Social Network
06	2022-02-12 13:07:18	10.0.027	oracle-db	Admin	shopify.com	0.0.42.67	Business Services
06	2022-02-12 13:07:18	10.0.027	oracle-db	Admin	slack.com	0.0.8.876	Technology and Computer
06	2022-02-12 13:07:18	10.0.0.27	oracle-db	Admin	beatingcorona.com	0.0.0.0	Malware/Virus
06	2022-02-12 13:07:18	10.0.027	oracle-db	Admin	facebook.com	0.0.34.23	Social Network
06	2022-02-12 13:07:18	10.0.027	oracle-db	Admin	dnssense.com	0.0.34.23	Technology and Computer
06	2022-02-12 13:07:18	10.0.027	oracle-db	Admin	shopify.com	0.0.34.23	Business Services
06	2022-02-12 13:07:18	10.0.027	oracle-db	Admin	google.com	0.0.34.23	Search Engines
06	2022-02-12 13:07:18	10.0.027	oracle-db	Admin	facebook.com	0.0.34.23	Social Networks
06	2022-02-12 13:07:18	10.0.027	oracle-db	Admin	google.com	0.0.34.23	Search Engines
06	2022-02-12 13:07:18	10.0.027	oracle-db	Admin	beatingcorona.com	0.0.34.23	Technology and Computer

Figure 5: A malicious domain without an IP address

The MITRE ATT&CK matrix began with an internal project called the FMX (Fort Meade Experiment). This tasked security experts to simulate hostile TTP against the network, and then collected and analyzed data on attacks against it. This data later formed the basis for ATT&CK. Because the ATT&CK matrix is a fairly complete description of attacker behaviour when hacking networks, the matrix is useful for various attack and defence dimensions, appearance models, and other mechanisms (e.g., FSTEC threat modelling).

MITRE has divided ATT&CK into several summary matrices: - Enterprise - TTP used in attacks against organizations; - TTP related to mobile and wearable devices; - ICS - industrial control systems, and TTP for industrial systems.

Each of the above tactics and techniques is related to the subject of this matrix. The most popular matrix is Enterprise. In turn, it consists of different parts, each of which has its responsibility:

- PRE matrix
- Windows
- macOS
- Linux
- Cloud
- Network
- Mobile

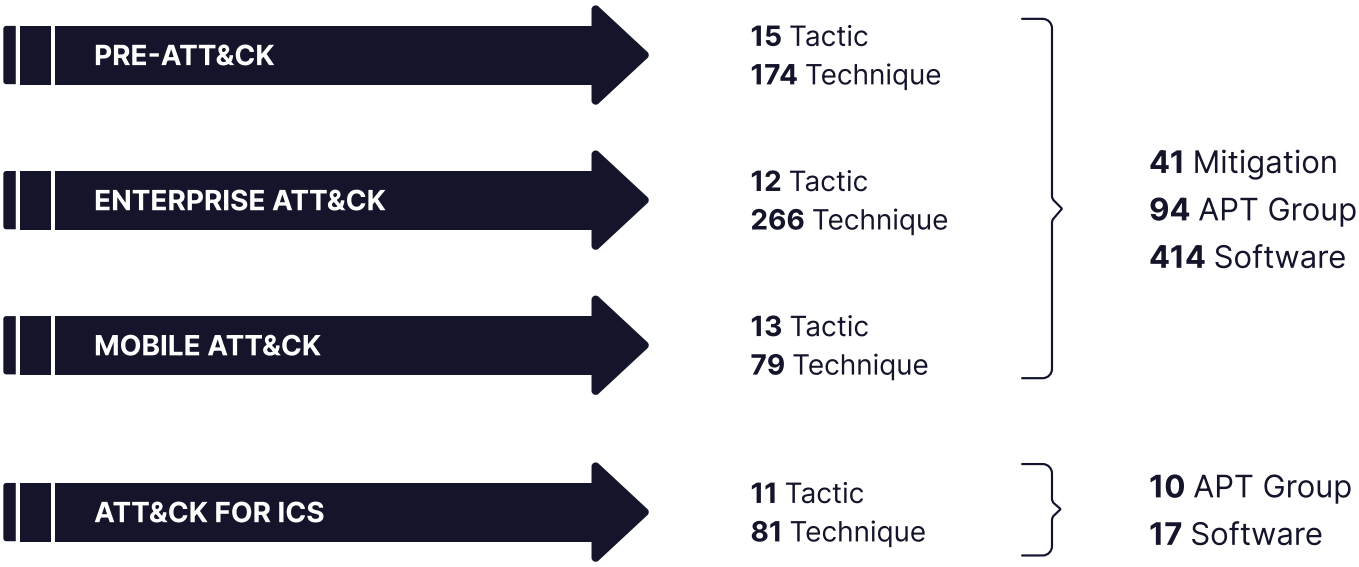


Figure 6: ATT&CK matrices

There are 3 basic types of attacks. Access to information is granted in groups.

PRE-ATT&CK

Priority Defination (Planning, Direction)
Target Selection
Information Gathering (Technical, people, organizational)
Weakness Identification (Technical, people, organizational)
Adversary OpSec
Establish & Maintain Infrastructure
Persona Development
Build Capabilities
Test Capabilities
Stage Capabilities

ENTERPRISE ATT&CK

Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Extrafiltration
Command and Control

Figure 7: Cyber Kill Chain mapped to MITRE PRE-ATT&CK and ATT&CK

The Pre-ATT&CK matrix includes gathering information, planning, identifying vulnerabilities and testing the planned plan. It is the process of responding to the actions in the ATT&CK framework in the organisation's ATT&CK matrix after the compromise.

Figure 8: ATT&CK Enterprise matrix for the Kill Chain model

For What Purposes Can the MITRE Be Used?

- Threat modelling
- Risk assessment related to security vulnerabilities
- Red/blue team exercises
- Preparation of defence plans
- Sharing cyber threat information
- Product testing, assessment
- Training of SOC teams
- See attack groups

Let's examine DNS infrastructure attacks with examples, using MITRE ATT&CK techniques and procedures.

Example-1 DNS Spoofing / Cache Poisoning

The example gives a description and motivation for the tactic. It has been said that attackers can use this tactic to compromise third-party DNS servers that can be used during the attack, and during post-invasion activities, attackers can use DNS traffic for various tasks, including command and control (e.g., Application Layer Protocol).

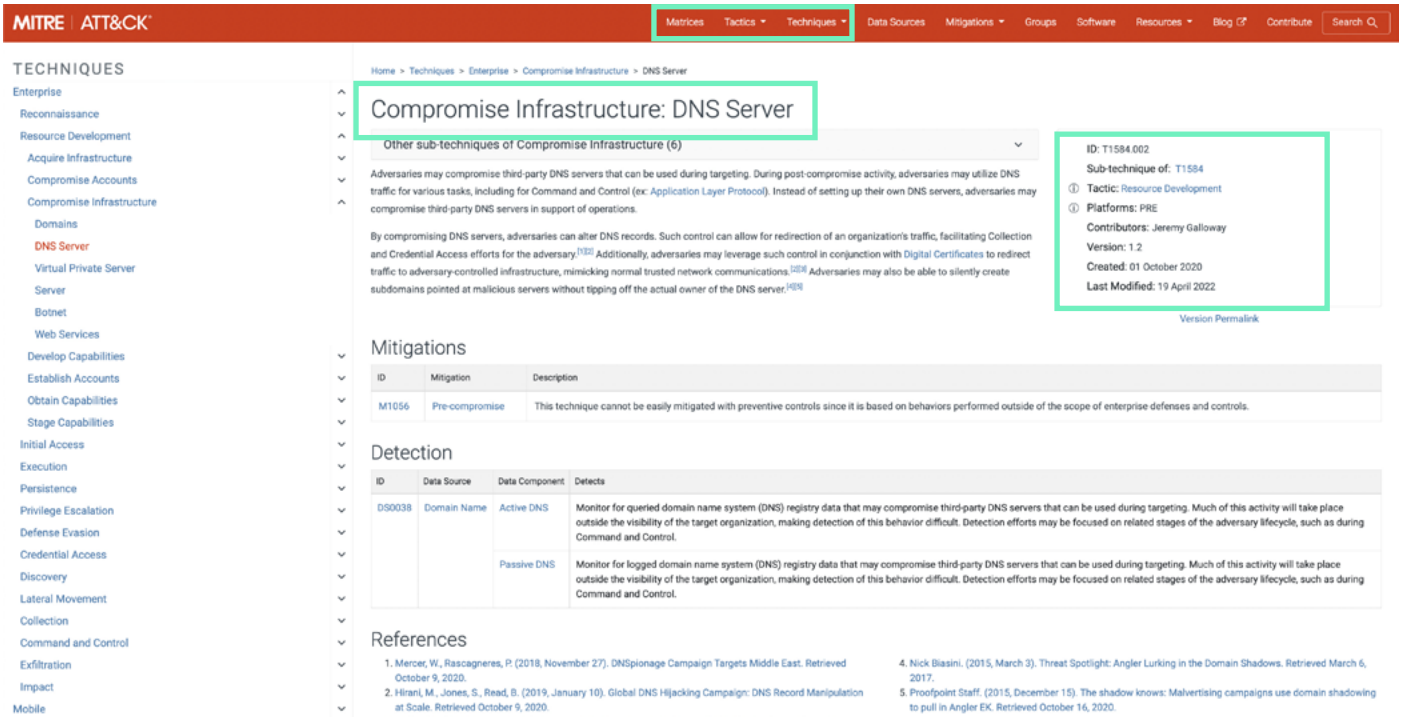


Figure 9: DNS Server ATT&CK technique in MITRE

In the second part, detailed information such as ID, on which platform it can be used, version, creation date and modification date are provided for quick access.

- **DNS SPOOFING**

1) attackers try to inject a spoofed address into the DNS

2) if the server accepts a spoofed address, the cache is sent

3) the requests are then processed by the attacker's server

DNS spoofing is a type of cyberattack in which an attacker redirects the victim's traffic (instead of a legitimate IP address) to a malicious website. Attackers use DNS cache poisoning to intercept Internet traffic and steal credentials or confidential information. DNS cache poisoning and spoofing are identical terms that are often used interchangeably.

Example-2 DNS Layer Security Threats (DNS tunnelling)

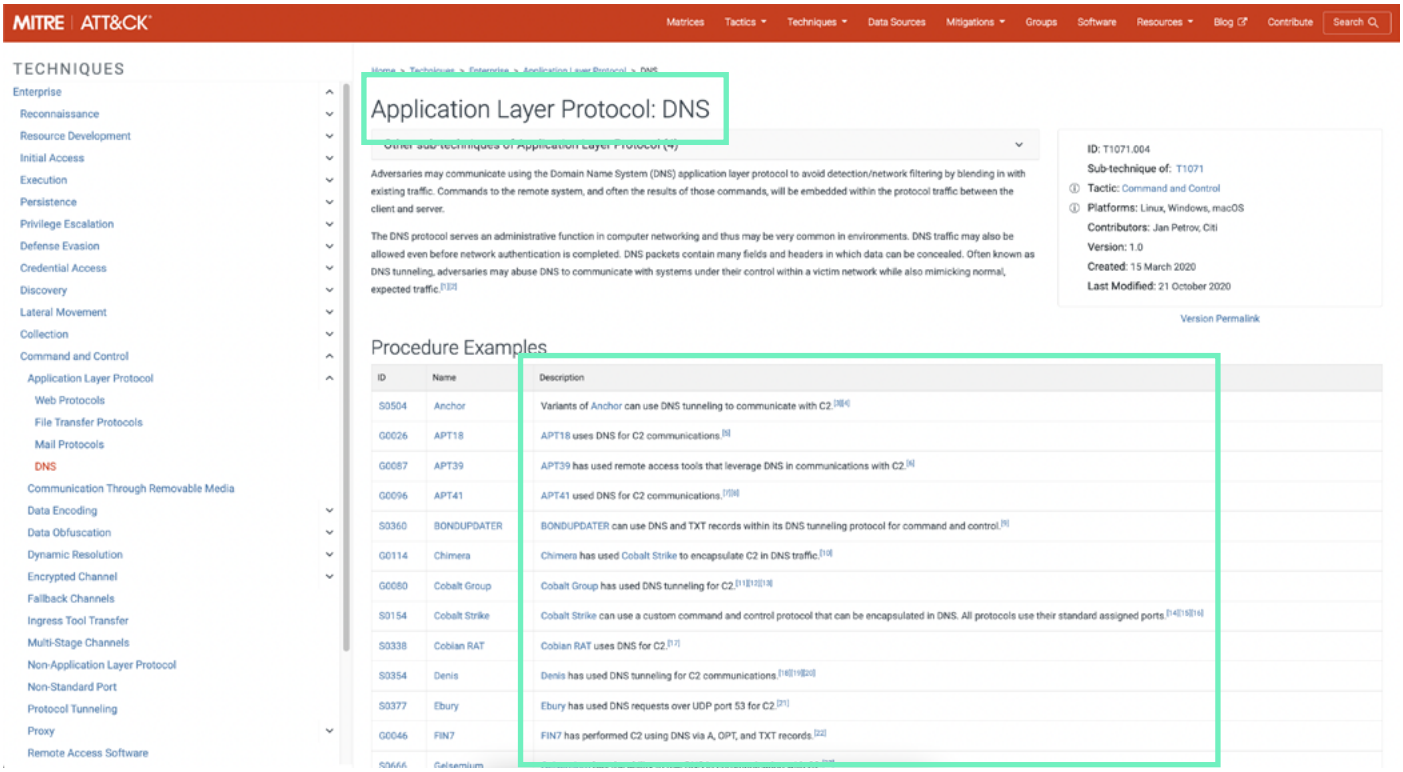


Figure 10: DNS Tunnelling attack technique and procedures

The attackers' attacks, examples of procedures, and explanations are detailed at MITRE.

• WHAT IS DNS TUNNELING

Web browsing, email, active directory, etc. All sorts of different services, such as using the Domain Name System (DNS) protocol to convert IP addresses into human-readable names. DNS was never used for data transmission, but for years it was intended to be used for that purpose by malicious people.

Cunning hackers realised that it was possible to secretly communicate with the victim's computer by injecting control commands and malicious data into the DNS protocol. This is the basic idea behind the DNS tunnel.

Mostly used to bypass network security controls for **data exfiltration** and **C2 communication** Tunnel protocols such as HTTP, FTP, and SSH over DNS.

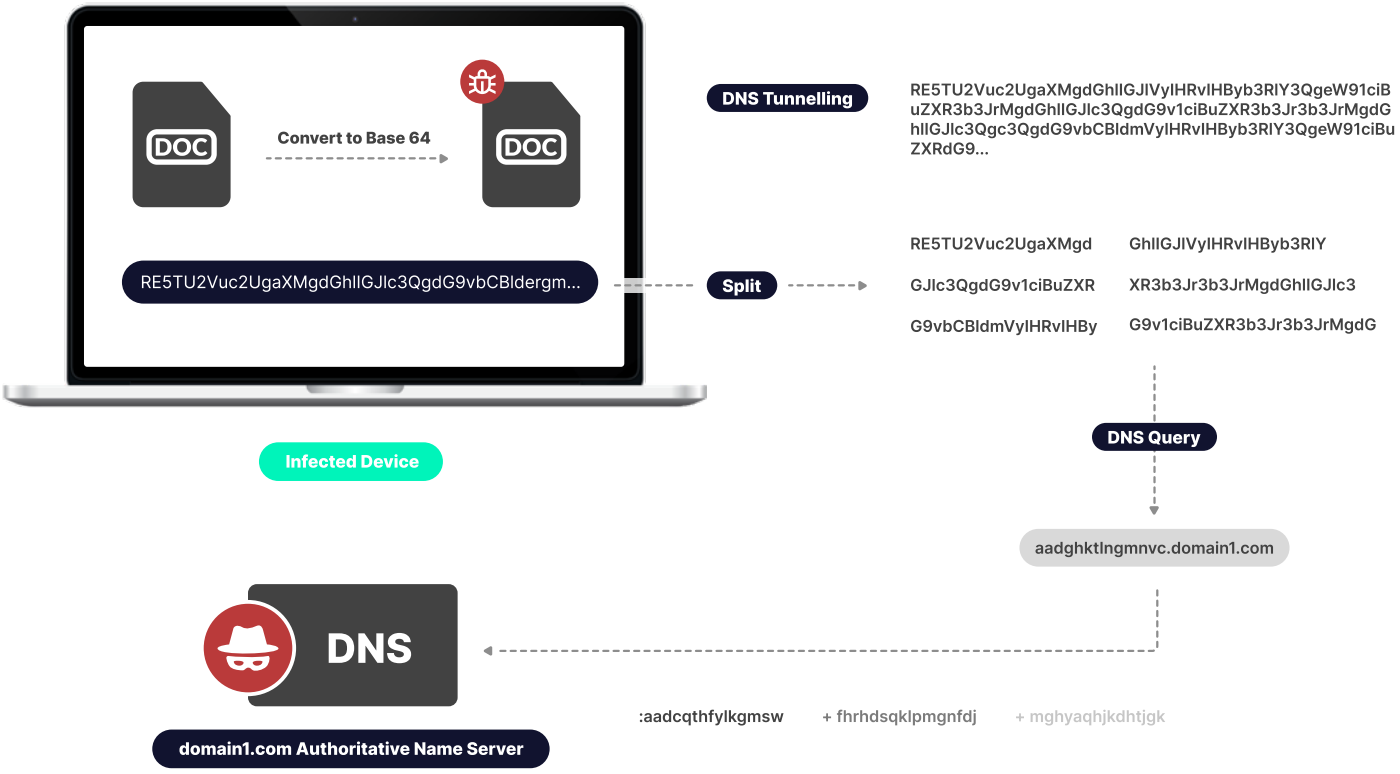


Figure 11: DNS Tunneling

The DNS tunnel detection and prevention module is part of the DNSSense Secure DNS cloud platform and is one of the features it offers. With this module, any DNS tunnelling attack activity is detected, blocked and reported very quickly, before any information about the file reaches the malicious attacker or the target it is directed to. Thus, data leaks are completely prevented.

DNS tunnelling is the attackers' preferred method of data theft, as it is almost undetectable by data loss protection products, other application-level security products, or network security teams to grab the important corporate data at their targets.

Example-3 DGA Domains

These are domains that are created with a certain algorithm according to the system clock. These domains are registered only when the zombie network is commanded and has the IP address. The owner of the zombie army has two goals:

- Preventing the command centre connection domains from being discovered by security researchers.
- Unlocking the zombie army on a temporal basis.

14	gtlhy.com	DGA Domain	0.0.0.0	64	0.04%
15	yxxxhj.com	DGA Domain	0.0.0.0	63	0.04%
16	326861.com	DGA Domain	0.0.0.0	62	0.04%
17	hdcecd.com	DGA Domain	0.0.0.0	62	0.04%
18	hollyflicks.com	DGA Domain	0.0.0.0	62	0.04%
19	yixianwen.com	DGA Domain	0.0.0.0	63	0.04%
20	hnlx68.com	DGA Domain	0.0.0.0	60	0.04%
21	faextdom.bank	DGA Domain	0.0.0.0	59	0.04%
22	hbxnxsls.com	DGA Domain	0.0.0.0	57	0.03%
23	hbycjt.com	DGA Domain	0.0.0.0	57	0.03%
24	hxscjt.com	DGA Domain	0.0.0.0	57	0.03%
25	zgbmbi.com	DGA Domain	0.0.0.0	56	0.03%
26	cjjcx.com	DGA Domain	0.0.0.0	55	0.03%

Figure 12: IP number of the DGA domains 0.0.0.0

DGA malware family	Primary Function	DGA Classification
Bobax	C&C	Binary
Murofet	C&C	Binary
Sinowal (Torpig)	C&C	Binary
Zeus GameOver (V1, V2, V3)	C&C	Binary
NeverQuest	C&C	Binary
Ramdo	C&C	Binary
FlashBack	C&C	Binary
PushDo	C&C	Binary
InfoStealer Shiz	C&C	Binary
Dyre/Dyreza	C&C	Binary
Cryptolocker (Ransomware)	C&C	Binary

DGA malware family	Primary Function	DGA Classification
Ramnit	C&C	Binary
Expiro (Expiro Z)	C&C	Binary
Conficker (A, B, C)	C&C	Binary
CoreFlood	C&C	Binary
DorkBot (NGR)	C&C	Binary
Rovnix	C&C	Binary
RunForestRun (All variants)	Infection	Script
Cridex or Dridex or Bugat	C&C	Binary
Tinba	C&C	Binary
Matsnu (Ransomware)	C&C	Binary
DNS Changer	C&C	Binary

Figure 13: DGA malware family and functions

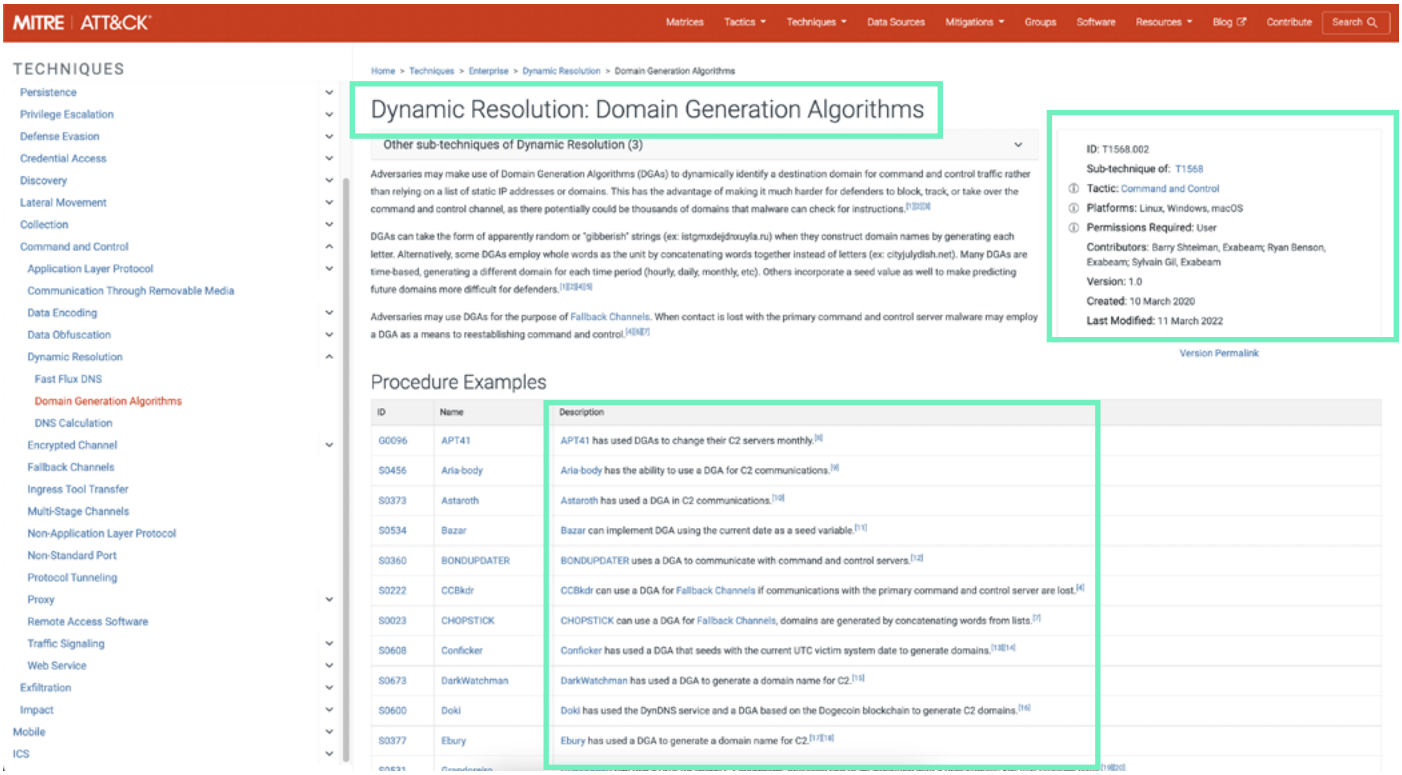


Figure 14: Mitre Frameworkunde Domain Generation Algorithms

It is given with **T1568.002** technique in DGA Mitre and procedure examples, mitigations detection method (Detection).

Domain generation algorithms (DGAs) allow attackers to manage websites to spread infections and command-and-control (C&C) facilities by changing domain names promptly.

One of the scenarios for using DGA can be observed when a computer system is infected with malware. Malware on a compromised machine attempts to connect to systems under the attacker's control to receive commands or send back collected information.

Attackers use DGA to calculate the order of domains that infected computers try to connect to. This is done to prevent control of the compromised infrastructure from being lost when the attacker's domains or IP addresses written directly into the code are blocked by security systems.

Example-4 PunyCode / Homoglyphic Attacks

A homoglyph attack is a deception technique that uses homoglyphs or homographs, in which an attacker abuses the similarity of character scripts to create **fake domains of existing brands to trick users into clicking.**

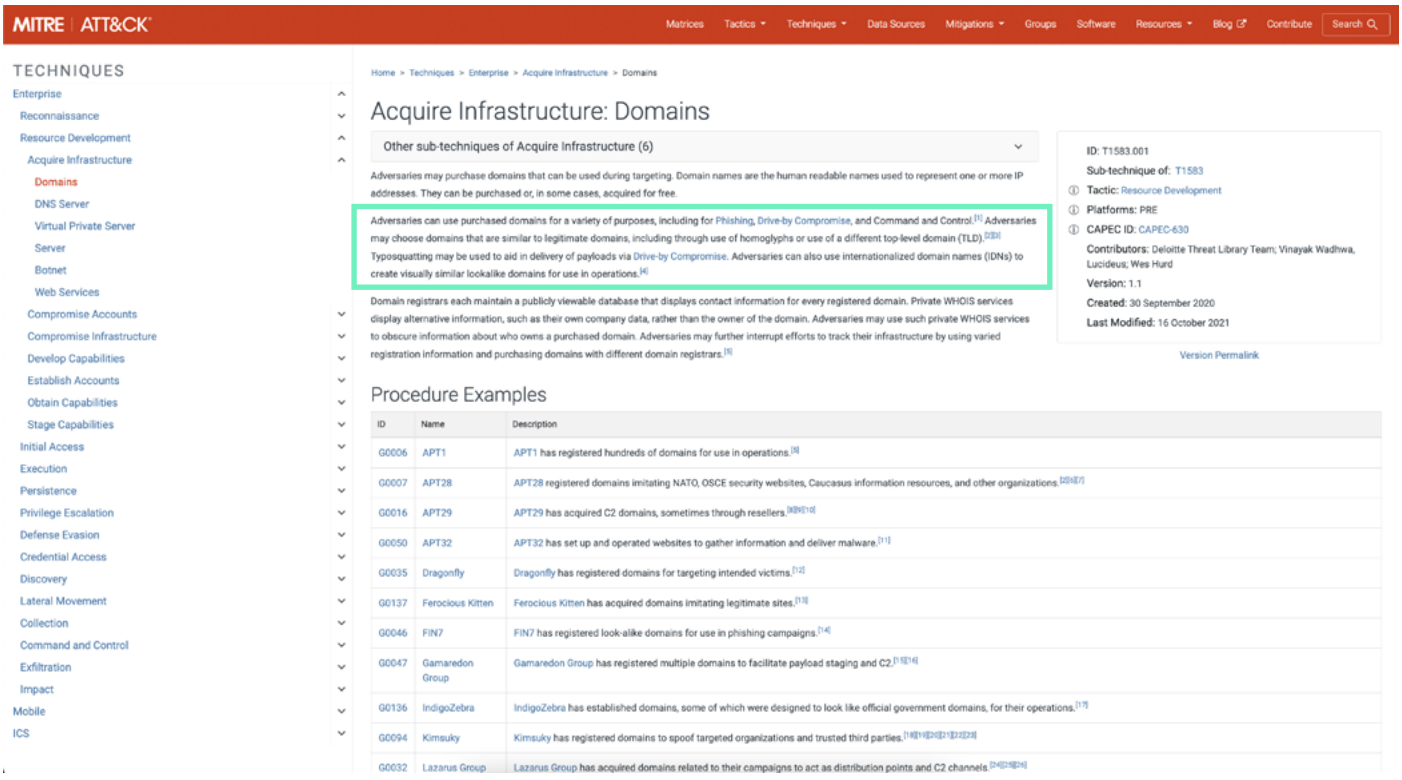


Figure 15: Punycode / Homoglyph Attacks technique in MITRE

One of the most important components users can use to determine if a URL is part of a phishing attack is to compare the host and domain name to what is expected of a legitimate website. For example, an email asking users to enter their banking information on a website with the domain name attackeradgh.com will not receive as many entries as a website hosted under a more reasonable-looking name. There are many common techniques used today and in the past to make links look more reputable. One of them, for example, would be **to have the anchor text say something else, but point to something else:**

```
<a href="http://attackeradghb.com">http://www.microsoft.com</a>
```

Another technique is **to confuse users by changing the URL so that the actual hostname is in the last part:**

```
http://www.microsoft.com@attackeradghb.com
```

Although some modern browsers give a warning, this can be circumvented by using Punycode and homoglyphic techniques.

Normally, DNS tags (parts separated by periods) should be contained only in the ASCII subset of letters, numbers, and a hyphen (sometimes called the LDH rule). In addition, a tag must not begin or end with a hyphen and is not case sensitive. This limited character set causes problems if someone wants to use a character in a DNS tag that is not part of the LDH set.

Punycode, or the International Domain Names in Applications (IDNA) framework used on the Internet, was developed to convert normally invalid characters in DNS hostnames into valid characters. In this way, domain and host names can be created using characters from a user's native language, but still, need to be translated into something the DNS system can use (assuming the application supports IDNA decoding). For example:

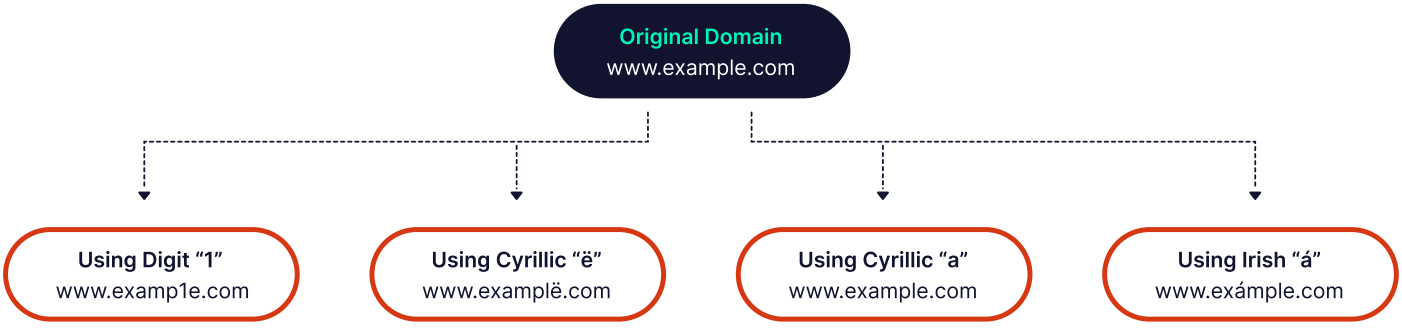
"https://kueche.de" (browsers that support the IDNA specification translate it to "https://xn--kche-0ra.de/". Not ASCII, for example, "HTTP:// 已从本地。中國" (these changes to the domain http://xn--1lq90ic7fzpc.xn--fiqz9s).

The second aspect of this attack is homoglyphs. A homoglyph is a symbol that looks the same or very similar to another symbol. An example that most people are familiar with is the letter O and the number 0. Depending on the font used, it can be difficult to tell them apart. The letters l (lowercase L) and I (uppercase i) are other common examples.

It gets even more interesting when there are very similar characters from different languages in Unicode. Languages that use diacritical accents, letter-like symbols, and other usable homoglyphs, and characters that look like the regular Latin alphabet show up with great regularity, some of them appearing to be almost exact copies of the same symbol. A common example is the Cyrillic alphabet, with very similar homoglyphs for a, c, e, o, p, x, and y. Even the Latin alphabet appears twice in Unicode.

Characters : !"$%&'()*+,-./0123456789:; < = >?@
ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_' abcdefghijklmnopqrstuvwxyz{|}~

It is represented in both the 0021-007E (Basic Latin) and FF01-FF5E (Full-width Latin) ranges of Unicode. This means that switching from one encoding to the other for a given Latin character is as easy as adding 65248 decimal values to the subrange versions. Depending on the font used, mixing character families can result in a "ransom note"-like visual effect. Example:



While IDNA is used to enable internationalized DNS tags, it can also be used to make a URL or hostname look more legitimate than it actually is. The Unicode representation can cause visual confusion for a user or inspire confidence where it should not. Example:

http://www.microsoft.com/index.html.attackeradghb.com may look like a legitimate Microsoft URL, but on closer inspection, it leads to a website that the author controls.

This is because the third slash symbol is not a slash symbol. The actual DNS record looks like this: microsoft.xn--comindex-g03d.html. attackeradghb.com

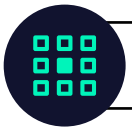
Details, examples of Punycode / Homoglyph Attacks technique in MITRE and examples of groups using it are given.

Two Important Components of the DNS Safety Concept

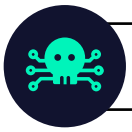
1) Ensuring the overall integrity and availability of DNS services that resolve hostnames on the network to IP addresses.

2) Monitoring DNS activity to detect potential security problems anywhere on your network.

Lack Protection Tools for DNS Layer Security Threats



Logs Not Centralized for Analysis



Even If You Have Logs, They Are Not Sufficient to Identify Security Threats

Signature / Indicator Driven Analysis are not enough

Manuel Deep Processing of DNS Logs is slow and cost prohibitive

Conclusion

MITRE ATT&CK is a powerful open source tool for understanding and classifying cyber attacker tactics, techniques, and procedures. MITRE has made it easy to improve cyber defence by providing a unified classification for classifying attackers and their behaviours in a consistent and easily communicated manner. Cyber defence teams can design a comprehensive strategy for security controls against potential threats and design tactics and techniques that attackers will display, assess risks, and then prioritize and address gaps in their cyber defences.

As DNSSense, we have explained DNS-specific usage in this whitepaper using the MITRE ATT&CK structure. We have focused on DNS analysis and Advanced DNS Visibility products for enterprise network needs. Today, we provide all the DNS analysis data that SOC teams need while ensuring that institutions are securely connected to the Internet with three integrated products.

Effectively monitoring DNS traffic on your network for suspicious anomalies is critical for the early detection of security breaches. With a tool like DNSSense Visibility, you'll be able to keep an eye on all the important metrics. With intelligent SIEM integration, you can set up alerts for a specific period or as a result of a combination of anomalous actions. DNSSense's artificial intelligence algorithms ensure over 99.5% classification. Based on this database, only the data that SOC teams need to review is sent to SIEM. This allows you to save over 95% of DNS log processing costs with intelligent SIEM integration.

References

- https://attack.mitre.org/groups/
- https://www.nist.gov/cyberframework
- https://detect-respond.blogspot.com/
- https://www.iso.org/isoiec-27001-information-security.html
- https://en.wikipedia.org/wiki/Mitre_Corporation
- http://www.ietf.org/rfc/rfc3492.txt

DNSSense
Easiest way to be secure

338a Regents Park Road, Office 3 And 4, N3 2LN London, United Kingdom

+44 (0) 203 376 03 30

info@dnssense.com