



SEPTEMBER 2022

WHITEPAPER

DNS LAYER SECURITY

FROM THE MITRE ATT&CK PERSPECTIVE

TABLE OF CONTENTS

● WHAT IS MITRE ATT&CK FRAMEWORK?	3
● WHY DO WE NEED MITRE ATT&CK?	4
● WHAT IS ATT&CK?	5
IOC (INDICATOR OF COMPROMISE) IOA (INDICATOR OF ATTACK)	6
ATT&CK MODEL	6
ATT&CK MODEL - TTP RELATIONSHIP	8
CYBER KILL CHAIN	8
● FOR WHAT PURPOSES CAN THE MITRE BE USED?	12
DNS SPOOFING / CACHE POISINING	12
DNS LAYER SECURITY THREATS (DNS TUNNELLING)	14
DGA DOMAINS	16
PUNYCODE / HOMOGLYPHIC ATTACKS	18
TWO IMPORTANT COMPONENTS OF THE DNS SECURITY CONCEPT	21
● CONCLUSION	22
REFERENCES	23

What is MITRE ATT&CK Framework?

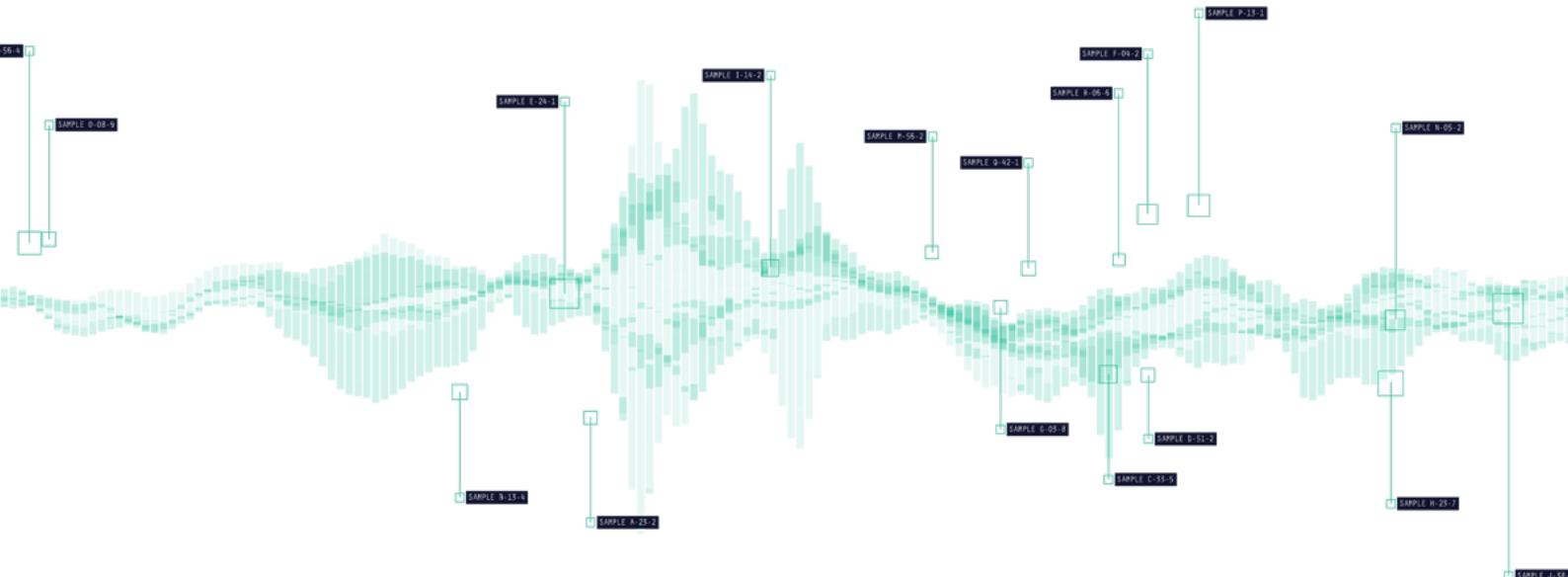
MITRE ATT&CK is one of the most popular methodologies among information security professionals. In the field of information security, MITRE Corporation is known for its CVE (Common Vulnerabilities and Exposures) list cve.mitre.org. This is a database of known vulnerabilities that was launched in 1999 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.



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).

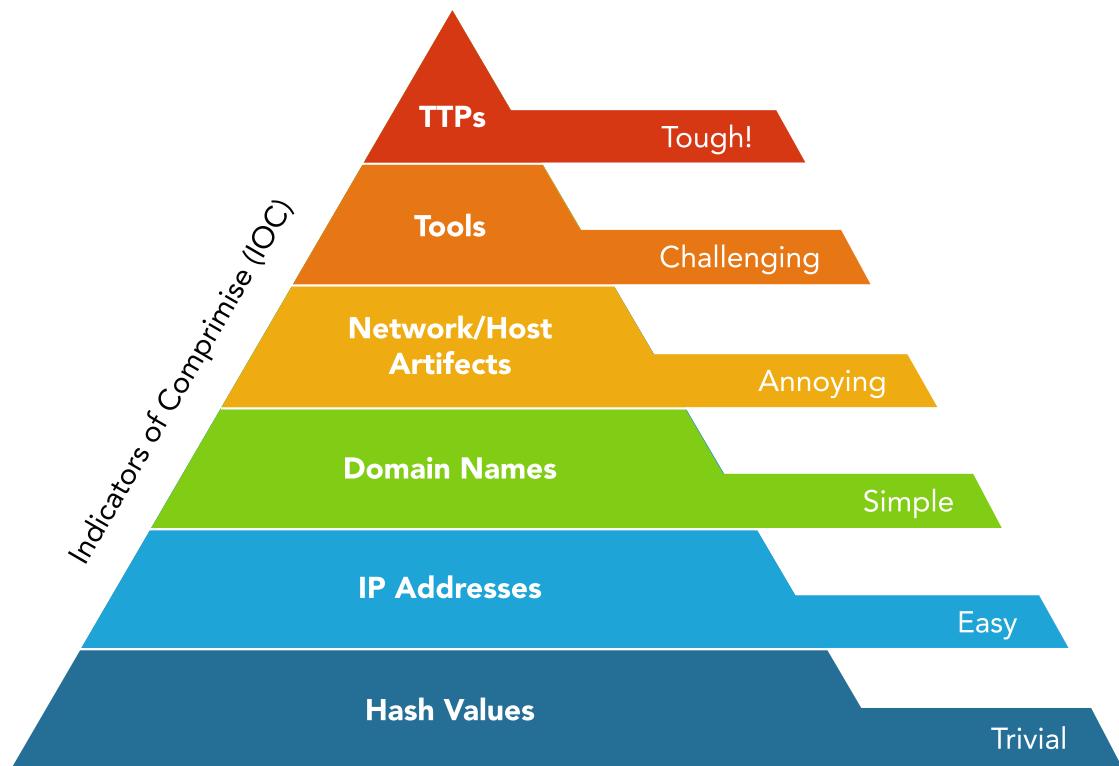
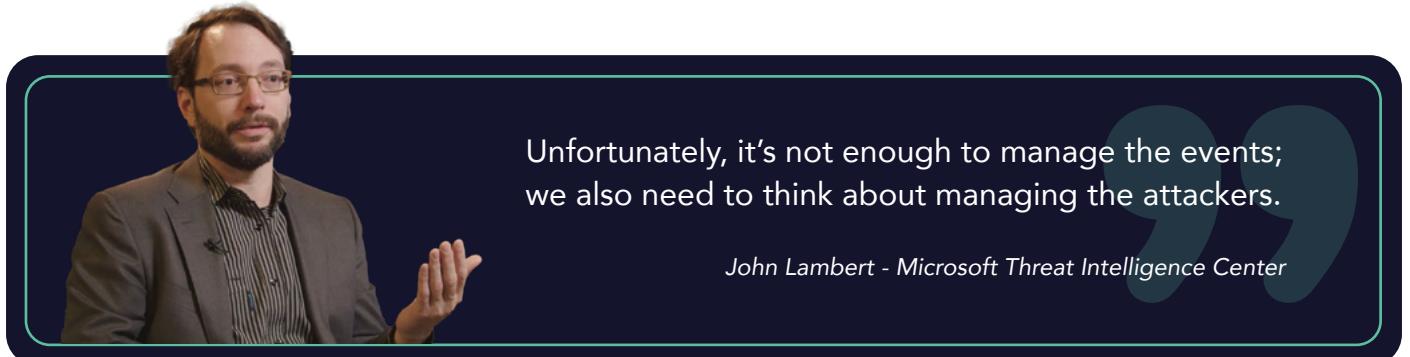


Figure 1 : David Bianco pyramid of pain

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 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:

TACTIC	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
TECHNIQUE	Drive-by Compromise	AppleScript	.bash_profile and .bachrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS_Jobs	Bash_History	Application Window	Application Deployment	Automated	Data Compressed	Communicate Through Removable Media	
Hardware Additions	Command Line Interface	AppCert DLLs	AppCert DLLs	Bi...	Bi...	Bi...	Bi...	Bi...	Data Encrypted	Connection Proxy	
Replication Through Removable Media	Control Panel Items	Applnit DLLs	Bypass User Account Control	Bi...	Bi...	Bi...	Bi...	Bi...	Data Transfer Size Limits	Custom	

Drive-by Compromise

A drive-by compromise is when an adversary gains access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is targeted for exploitation. This can happen in several ways, but there are a few main components:

Multiple ways of delivering exploit code to a browser exist, including:

- A legitimate website is compromised where adversaries have injected some form of malicious code such as JavaScript, iFrames, cross-site scripting.
- Malicious ads are paid for and served through legitimate ad providers.
- Built-in web application interfaces are leveraged for the insertion of any other kind of object that can be used to display web content or contains a script that executes on the visiting client (e.g. forum posts, comments, and other user controllable web content).

Often the website used by an adversary is one visited by a specific community, such as government, a particular industry, or region, where the goal is to compromise a specific user or set of users based on a shared interest. This kind of targeted attack is referred to as a strategic web compromise or watering hole attack. There are several known examples of this occurring.^[1]

Drive-by Compromise	
ID	T1189
Tactic	Initial Access
Platforms	Linux, Windows, macOS
Permissions	User
Delivery	Packet capture, Network device logs, Process use of network, Web proxy, Network intrusion detection system, SSL/TLS inspection
Sources	

PROCEDURE

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.

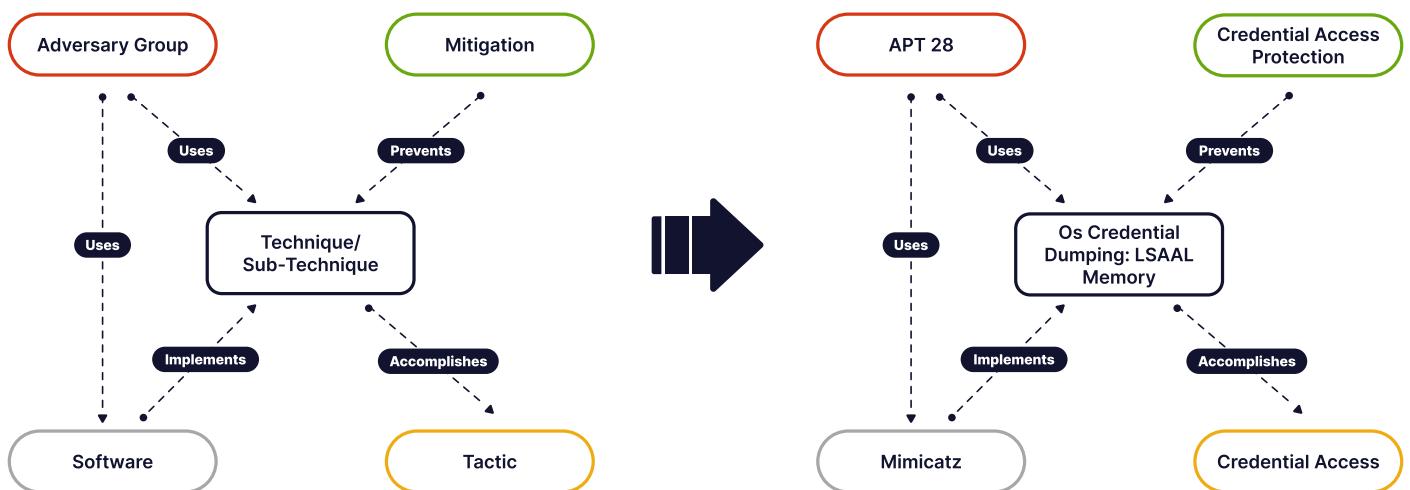


Figure 3 : ATT&CK model – TTP relationship

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.

#	Time	Source				Destination			Decision	
		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

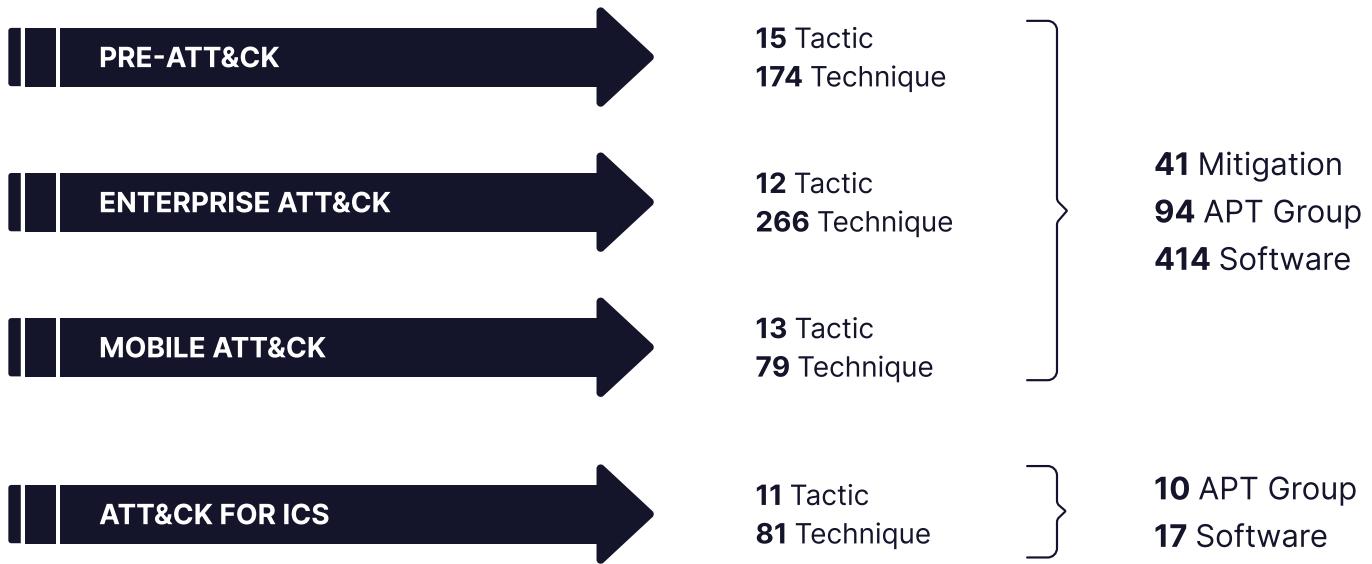


Figure 6: ATT&CK matrices

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

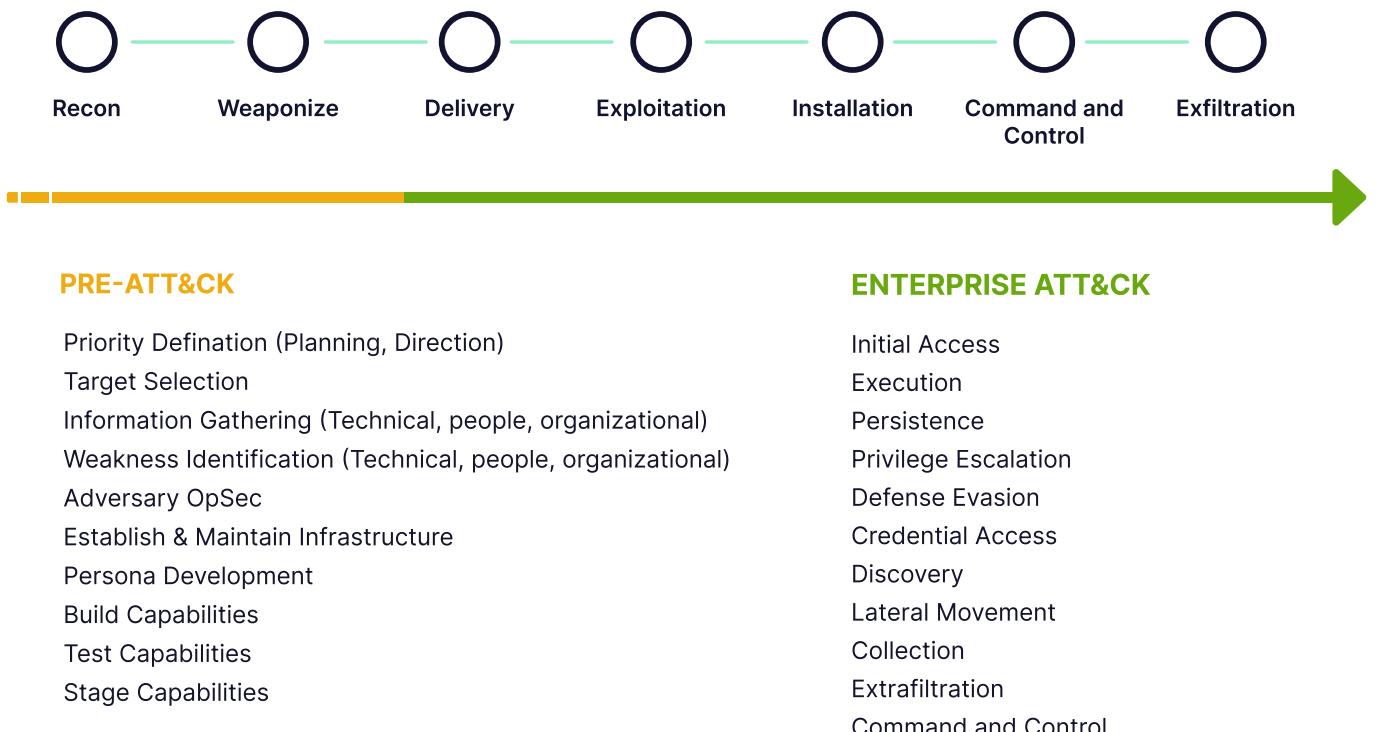


Figure 7: Cyber Kill Chain mapped to MITRE PRE-ATT&CK and ATT&CK

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](#)).

Compromise Infrastructure: DNS Server

Mitigations

ID	Mitigation	Description
M1056	Pre-compromise	This technique cannot be easily mitigated with preventive controls since it is based on behaviors performed outside of the scope of enterprise defenses and controls.

Detection

ID	Data Source	Data Component	Detected
DS0038	Domain Name	Active DNS	Monitor for queried domain name system (DNS) registry data that may compromise third-party DNS servers that can be used during targeting. Much of this activity will take place outside the visibility of the target organization, making detection of this behavior difficult. Detection efforts may be focused on related stages of the adversary lifecycle, such as during Command and Control.
		Passive DNS	Monitor for logged domain name system (DNS) registry data that may compromise third-party DNS servers that can be used during targeting. Much of this activity will take place outside the visibility of the target organization, making detection of this behavior difficult. Detection efforts may be focused on related stages of the adversary lifecycle, such as during Command and Control.

References

- 1. Mercer, W., Rascagneres, P. (2018, November 27). DNSpionage Campaign Targets Middle East. Retrieved October 9, 2020.
- 2. Hirani, M., Jones, S., Read, B. (2019, January 10). Global DNS Hijacking Campaign: DNS Record Manipulation at Scale. Retrieved October 9, 2020.
- 4. Nick Biasini. (2015, March 3). Threat Spotlight: Angler Lurking in the Domain Shadows. Retrieved March 6, 2017.
- 5. Proofpoint Staff. (2015, December 15). The shadow knows: Malvertising campaigns use domain shadowing to pull in Angler EK. Retrieved October 16, 2020.

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)

The screenshot shows the MITRE ATT&CK framework interface. On the left, there's a navigation tree under the 'TECHNIQUES' heading, which includes categories like Reconnaissance, Persistence, and Command and Control. The main content area is titled 'Application Layer Protocol: DNS'. It contains a brief description of how DNS can be used for command and control, followed by a table titled 'Procedure Examples'. This table lists various techniques with their IDs and names, along with a detailed description of each. A specific row for 'DNS' is highlighted with a green border. The right side of the page provides technical details for this technique, including its ID (T1071.004), sub-technique (T1071), tactic (Command and Control), platforms (Linux, Windows, macOS), contributors (Jan Petrov, Citi), version (1.0), creation date (15 March 2020), and last modified date (21 October 2020). There's also a 'Version Permalink' link.

ID	Name	Description
G00504	Anchor	Variants of Anchor can use DNS tunneling to communicate with C2. ^{[28][29]}
G0026	APT18	APT18 uses DNS for C2 communications. ^[30]
G0087	APT39	APT39 has used remote access tools that leverage DNS in communications with C2. ^[31]
G0096	APT41	APT41 used DNS for C2 communications. ^{[32][33]}
G0360	BONDUPDATER	BONDUPDATER can use DNS and TXT records within its DNS tunneling protocol for command and control. ^[34]
G0114	Chimera	Chimera has used Cobalt Strike to encapsulate C2 in DNS traffic. ^[35]
G0080	Cobalt Group	Cobalt Group has used DNS tunneling for C2. ^{[36][37][38]}
S0154	Cobalt Strike	Cobalt Strike can use a custom command and control protocol that can be encapsulated in DNS. All protocols use their standard assigned ports. ^{[39][40][41]}
S0338	Cobian RAT	Cobian RAT uses DNS for C2. ^[37]
S0354	Denis	Denis has used DNS tunneling for C2 communications. ^{[42][43][44]}
S0377	Ebury	Ebury has used DNS requests over UDP port 53 for C2. ^[45]
G0046	FIN7	FIN7 has performed C2 using DNS via A, OPT, and TXT records. ^[22]
S0466	Galaximium	

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.

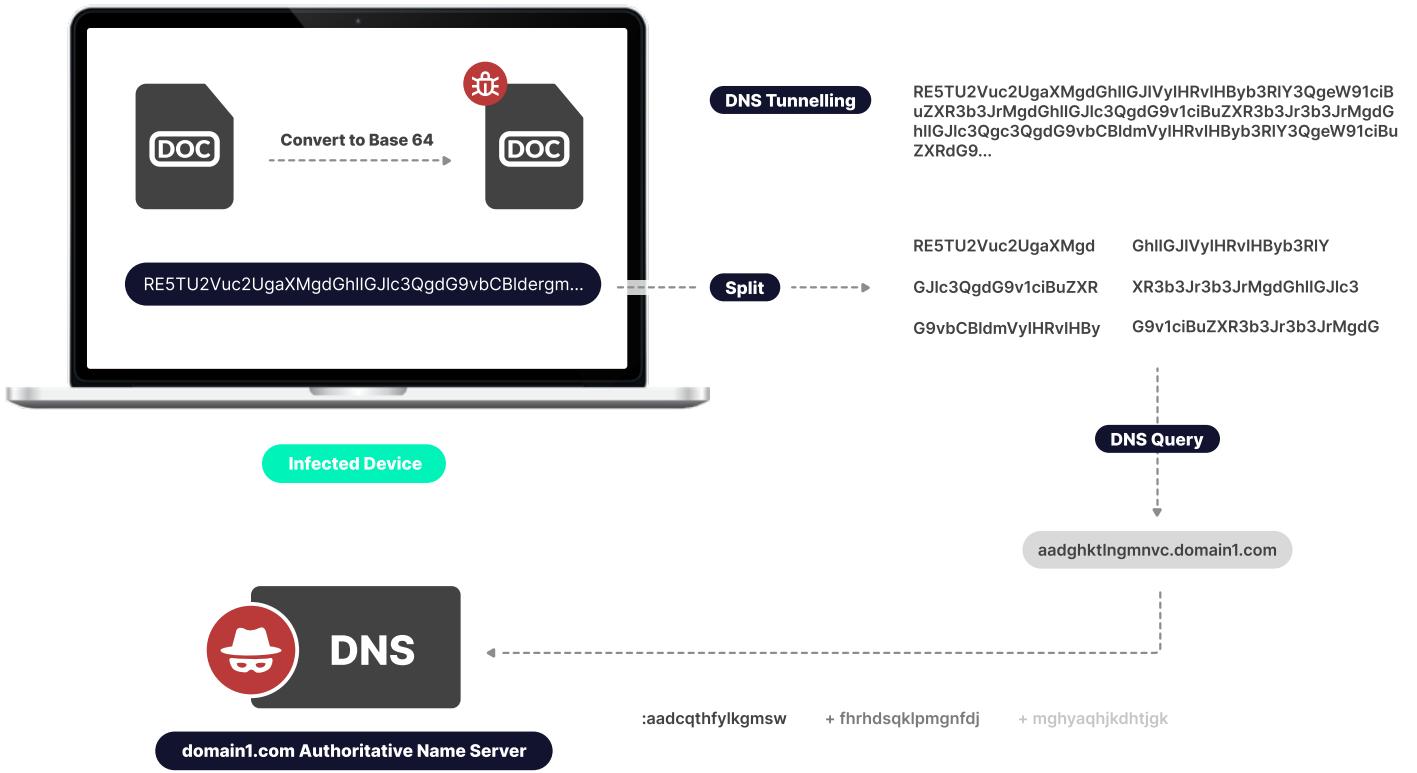


Figure 11: DNS Tunneling

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.



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

The screenshot shows the MITRE ATT&CK framework interface. On the left, there's a sidebar with a tree view of various techniques under the 'TECHNIQUES' heading. The main content area has a breadcrumb navigation path: Home > Techniques > Enterprise > Dynamic Resolution > Domain Generation Algorithms. The main title is 'Dynamic Resolution: Domain Generation Algorithms'. Below it, a sub-section titled 'Other sub-techniques of Dynamic Resolution (3)' is shown. A large green box highlights the 'Procedure Examples' section, which contains a table with columns for ID, Name, and Description. The table lists several DGA techniques used by different malware families. To the right of the table, another green box highlights the 'Details' section, which provides specific information about the technique, including its ID (T1568.002), sub-technique of (T1568), tactic (Command and Control), platforms (Linux, Windows, macOS), permissions required (User), contributors (Barry Shteman, Exabeam; Ryan Benson, Exabeam; Sylvain Gil, Exabeam), version (1.0), creation date (10 March 2020), and last modified date (11 March 2022). A 'Version Permalink' link is also present.

ID	Name	Description
G0096	APT41	APT41 has used DGAs to change their C2 servers monthly. ^[3]
S0456	Aria-body	Aria-body has the ability to use a DGA for C2 communications. ^[10]
S0373	Astaroth	Astaroth has used a DGA in C2 communications. ^[10]
S0534	Bazar	Bazar can implement DGA using the current date as a seed variable. ^[11]
S0360	BONDUPDATER	BONDUPDATER uses a DGA to communicate with command and control servers. ^[12]
S0222	CCBkdr	CCBkdr can use a DGA for Fallback Channels if communications with the primary command and control server are lost. ^[4]
S0023	CHOPSTICK	CHOPSTICK can use a DGA for Fallback Channels, domains are generated by concatenating words from lists. ^[5]
S0608	Conficker	Conficker has used a DGA that seeds with the current UTC victim system date to generate domains. ^{[13][14]}
S0673	DarkWatchman	DarkWatchman has used a DGA to generate a domain name for C2. ^[15]
S0600	Doki	Doki has used the DynDNS service and a DGA based on the Dogecoin blockchain to generate C2 domains. ^[16]
S0377	Ebury	Ebury has used a DGA to generate a domain name for C2. ^{[17][18]}

Figure 14: Mitre Frameworkkunde 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**.

The screenshot shows the MITRE ATT&CK framework interface. On the left, there is a sidebar titled 'TECHNIQUES' with a hierarchical tree view of various attack techniques. The 'Domains' node under 'Acquire Infrastructure' is expanded, and its sub-node 'Other sub-techniques of Acquire Infrastructure (6)' is also expanded. The main content area displays the details for 'Acquire Infrastructure: Domains'. At the top of this section is a heading 'Acquire Infrastructure: Domains' and a breadcrumb trail: Home > Techniques > Enterprise > Acquire Infrastructure > Domains. Below the heading is a sub-section titled 'Other sub-techniques of Acquire Infrastructure (6)'. A callout box highlights a paragraph about adversaries using purchased domains for various purposes, including Phishing, Drive-by Compromise, and Command and Control. To the right of the main content is a detailed sidebar with technical metadata: ID: T1583.001, Sub-technique of: T1583, Tactic: Resource Development, Platform: PRE, CAPEC ID: CAPEC-630, Contributors: Deloitte Threat Library Team, Vinayak Wadhwani, Lucideus, Wes Hurd, Version: 1.1, Created: 30 September 2020, Last Modified: 16 October 2021, and a 'Version Permalink' link. Below the sidebar is a table titled 'Procedure Examples' with 13 rows, each listing an ID, name, and description of an adversary's domain acquisition tactic.

ID	Name	Description
G0006	APT1	APT1 has registered hundreds of domains for use in operations. ^[1]
G0007	APT28	APT28 registered domains imitating NATO, OSCE security websites, Caucasus information resources, and other organizations. ^{[2][3]}
G0016	APT29	APT29 has acquired C2 domains, sometimes through resellers. ^{[4][5]}
G0050	APT32	APT32 has set up and operated websites to gather information and deliver malware. ^[6]
G0035	Dragonfly	Dragonfly has registered domains for targeting intended victims. ^[7]
G0137	Ferocious Kitten	Ferocious Kitten has acquired domains imitating legitimate sites. ^[8]
G0046	FIN7	FIN7 has registered look-alike domains for use in phishing campaigns. ^[9]
G0047	Gamaredon Group	Gamaredon Group has registered multiple domains to facilitate payload staging and C2. ^{[10][11]}
G0136	IndigoZebra	IndigoZebra has established domains, some of which were designed to look like official government domains, for their operations. ^[12]
G0094	Kimsuky	Kimsuky has registered domains to spoof targeted organizations and trusted third parties. ^{[13][14][15][16]}
G0032	Lazarus Group	Lazarus Group has acquired domains related to their campaigns to act as distribution points and C2 channels. ^{[17][18]}

Figure 15: Punycode / Homoglyphic 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:

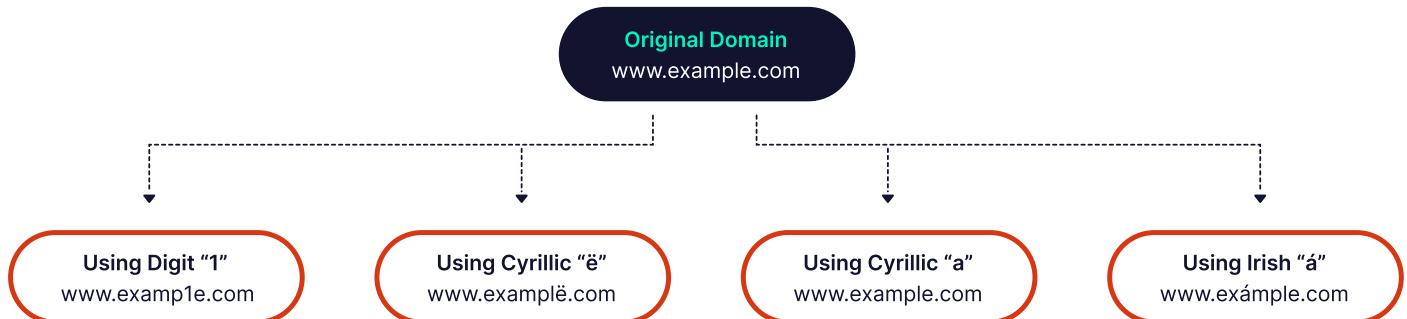
```
"https://kueche.de" (browsers that support the IDNA specification translate it to  
"https://xn--kche-0ra.de/". Not ASCII, for example, "HTTP:// 已从本地. 中國" (these  
changes to the domain http://xn--1lq90ic7fzpc.xn--fiqz9s).
```

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

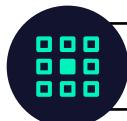
Details, examples of Punycode / Homoglyph Attacks technique in MITRE and examples of groups using it are given.

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



Manual 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>



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

© 2022 The Secureend LTD. DNSSense is registered trademark of Secureend LTD. MITRE, CVE, MITRE ATT&CK, ATT&CK are registered trademarks of The MITRE Corporation. All other trademarks, service marks and company names are properties of their respective owners.
© 2022 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation.