[redacted]

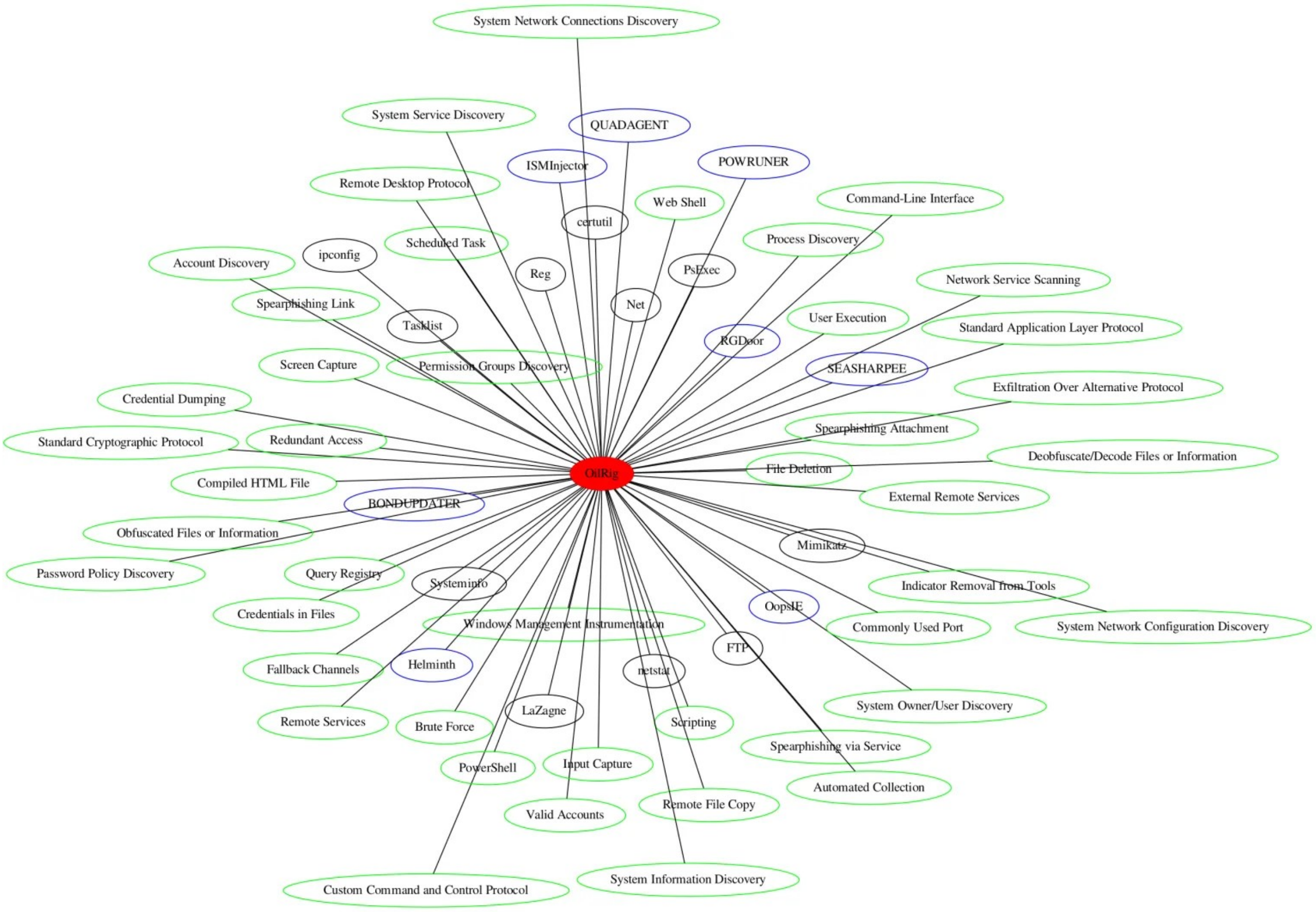
Iranian Threat Actors: Preliminary Analysis

APT, CYBERSECURITY, EXPERIENCE JANUARY 15, 2020

Nowadays Iran's Cybersecurity capabilities are under microscope, many news sites, gov. agencies and security experts warn about a possible cybersecurity infiltration from Iranian government and alert to increase cybersecurity defensive levels. Today I want to share a quick and short study based on cross correlation between **MITRE ATT&CK** and **Malpedia** about some of the main threat actors attributed to Iran. The Following sections describe the TTPs (Tactics, Techniques and Procedures) used by some of the most influential Iranian APT groups. Each section comes with a main graph which is built by scripting and which comes without legend, so please keep in mind while reading that: the **red** circles represent the analyzed threat actors, the **green** circles represent threat actor's used techniques, the **blue** circles represent the threat actor's used Malware and the **black** circles represent the threat actor's used tool sets.

OilRig

well. It also appears OilRig carries out supply chain attacks, where the threat group leverages the trust relationship between organizations to attack their primary targets.” The threat actor uses opensource tools such as **Mimikatz** and **laZagne**, common sysadmin toolset available on Microsoft distribution or sysinternals such as: PsExec, CertUtil, Netstat, SystemInfo, ipconfig and tasklist. Bonupdater, Helminth, Quadangent and PowRuner are some of the most sophisticated Malware attributed to OilRig and analyzed over the past few years. Techniques (green) are mainly focused in the lateral movements and in getting persistence on the victim infrastructure; few of them involved exploiting or 0days initiatives.

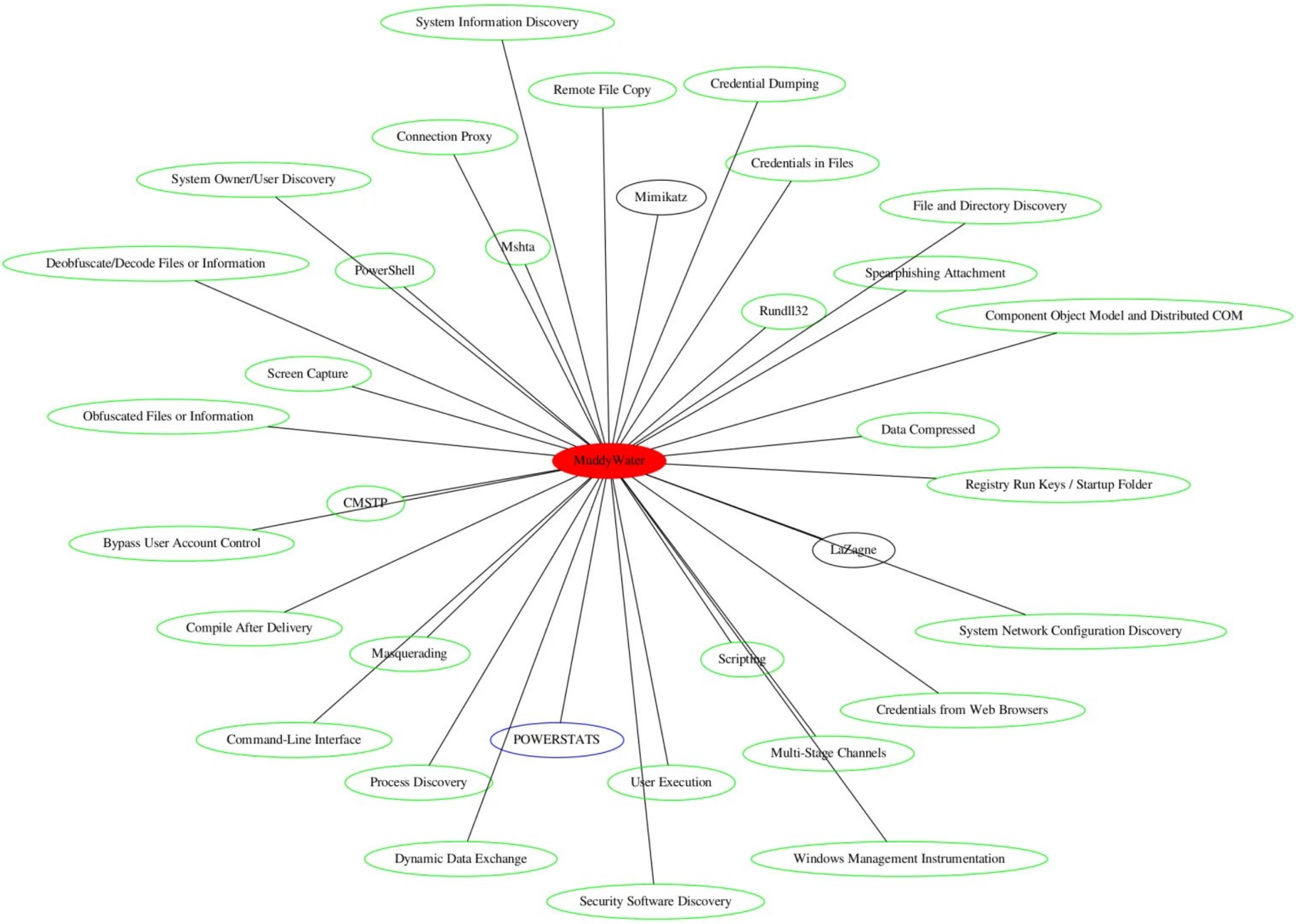


OilRig TTP

Those observations would suggest a powerful group mostly focused on staying hidden rather than getting access through advanced techniques. Indeed no 0days or usage of advanced exploits is found over the target infrastructure. If so we are facing a state-sponsored group with high capabilities in developing persistence and hidden communication channels (for example over DNS) but without a deep interest in exploiting services. This topic would rise a question: OilRig does not need advanced exploiting

MuddyWater

According to MITRE: “MuddyWater is an Iranian threat group that has primarily targeted Middle Eastern nations, and has also targeted European and North American nations. The group’s victims are mainly in the telecommunications, government (IT services), and oil sectors.” Currently we have few artifacts related to MuddyWater (‘Muddy’), indeed only Powerstats backdoor is actually attributed to it. Their attack are typically “hands driven”, which means they do not use automation lateral movement but they prefer to use opensource tools or sysinternal ones to deliberately move between target network rather than running massively exploits or scanners.

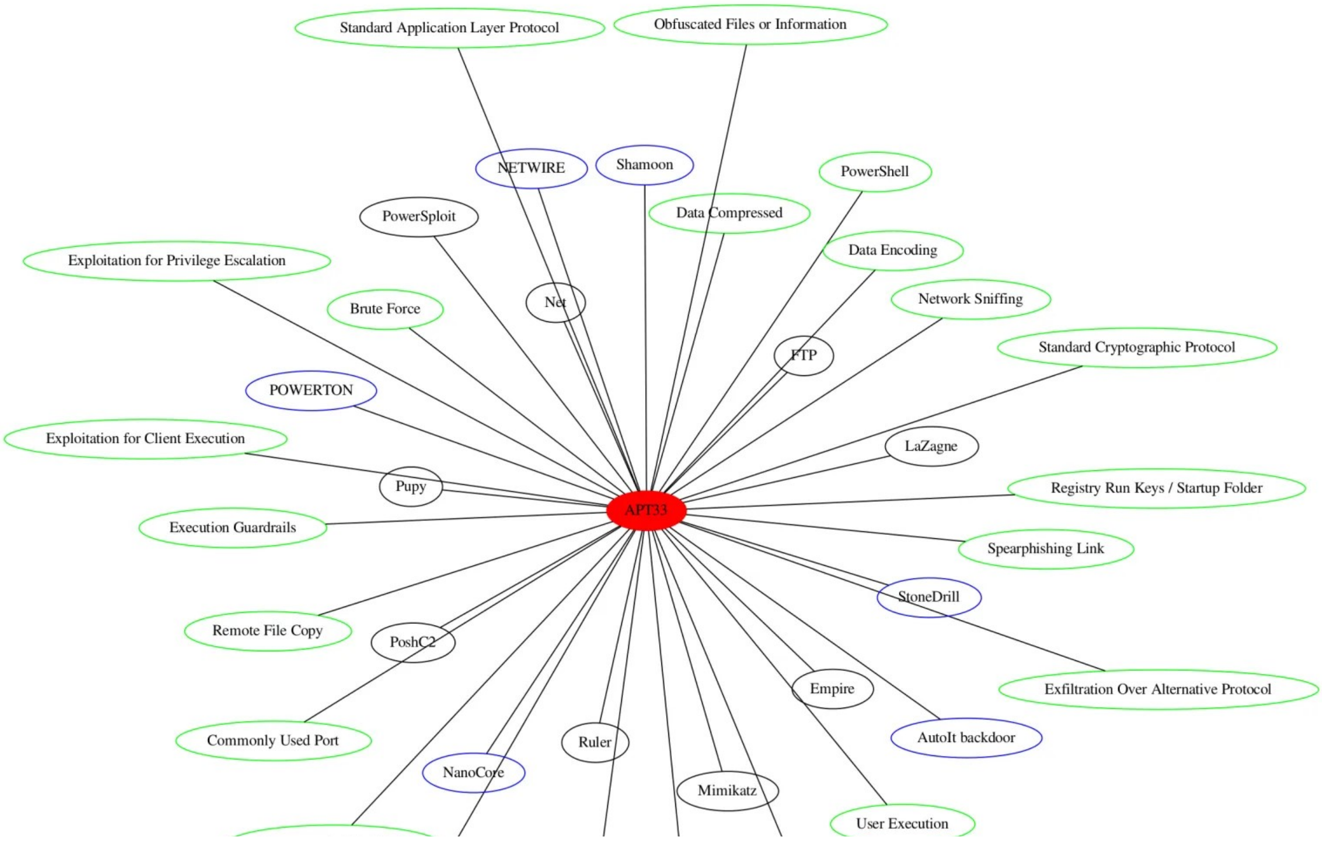

System Information Discovery
Remote File Copy
Credential Dumping
Connection Proxy
Credentials in Files
System Owner/User Discovery
Mimikatz
File and Directory Discovery
Mshta
Deobfuscate/Decode Files or Information
PowerShell
Spearphishing Attachment
Rundll32
Component Object Model and Distributed COM
Screen Capture
Obfuscated Files or Information
Data Compressed
MuddyWater
Registry Run Keys / Startup Folder
CMSTP
Bypass User Account Control
LaZagne
Compile After Delivery
System Network Configuration Discovery
Masquerading
Scripting
Credentials from Web Browsers
Command-Line Interface
POWERSTATS
Multi-Stage Channels
Process Discovery
User Execution
Dynamic Data Exchange
Windows Management Instrumentation
Security Software Discovery

MuddyWater TTP

Once landed inside a victim machine Muddy looks for local credentials and then moves back and forward by using such a credentials directly on the network/domain controllers. According to MITRE techniques (green) MuddyWater to take an entire target-network might proxies/nat.

APT33

According to MITRE: “APT33 is a suspected Iranian threat group that has carried out operations since at least 2013. The group has targeted organizations across multiple industries in the United States, Saudi Arabia, and South Korea, with a particular interest in the aviation and energy sectors.” Analyzing the observed TTPs we might agree that this threat actor looks very close to MuddyWater. If you take a closer look to the Muddy Graph (in the previous dedicated section) and APT33 graph (following) you will see many similarities: many tools are shared, many techniques are shared and even artifacts **Powerstats** (Muddy) and **Powertron** (APT33) share functions and a small subset of code (even if they have different code bases and differ in functionalities). We have more information about APT33 if compared to MuddyWatter, but similarities on TTPs could induce an avid reader to think that we might consider APT33 as the main threat actor while MuddyWater a specific ‘operation’ of the APT33 actor.



But if you wonder why I decided to keep them separated on such personal and preliminary analysis you could find the answer in the reason in why they do attack. APT33 showed destruction intents by using Malware such as **shamoon** and **stoneDrill**, while Muddy mostly wants to "**backdooring**" the victims.

CopyKittens

According to MITRE: "CopyKittens is an Iranian cyber espionage group that has been operating since at least 2013. It has targeted countries including Israel, Saudi Arabia, Turkey, the U.S., Jordan, and Germany. The group is responsible for the campaign known as Operation Wilted Tulip." CopyKittens threat actor actually differ from the previous ones. First of all we see the usage of CobaltStrike, which is an autonomous exploiting system (well actually is much more, but let me simplify it). Cobalt and Empire (a post exploitation framework) taken together would allow the attacker to automate lateral movement. Which is a damn different behavior respect to previous actors. CopyKittens would make much more noise inside an attacked network and would be easier to detect if using such automation tools, but on the other hand they would be much more quick in reaching their targets and run away.

CopyKittens TTP

One more characteristic is the "code signing". While in OilRig, MuddyWater and APT33 we mostly observed "scripting" capabilities, in CopyKittens we are observing most advanced code capabilities. Indeed code signing is used on Microsoft Windows and IOS to guarantee that the software comes from known developer and that it has not been tampered with. While a script (node, python, AutoIt) could be attribute to IT guys as well as developers, developing more robust and complex software (such as: java, .net, c++, etc) is a skill typically attributed to developers. This difference could be significant in suspecting a small set of different people working on CopyKittens.

Cleaver

evidence suggests Cleaver is linked to Threat Group 2889 (TG-2889). " We have few information about this group, and as you might see there are few similarities. The usage of Mimikatz could be easily adopted for credential dumping, while TinyZBot is a quite interesting tool since it mostly implements spying capabilities without strong architectural design or code execution or data exfiltration.

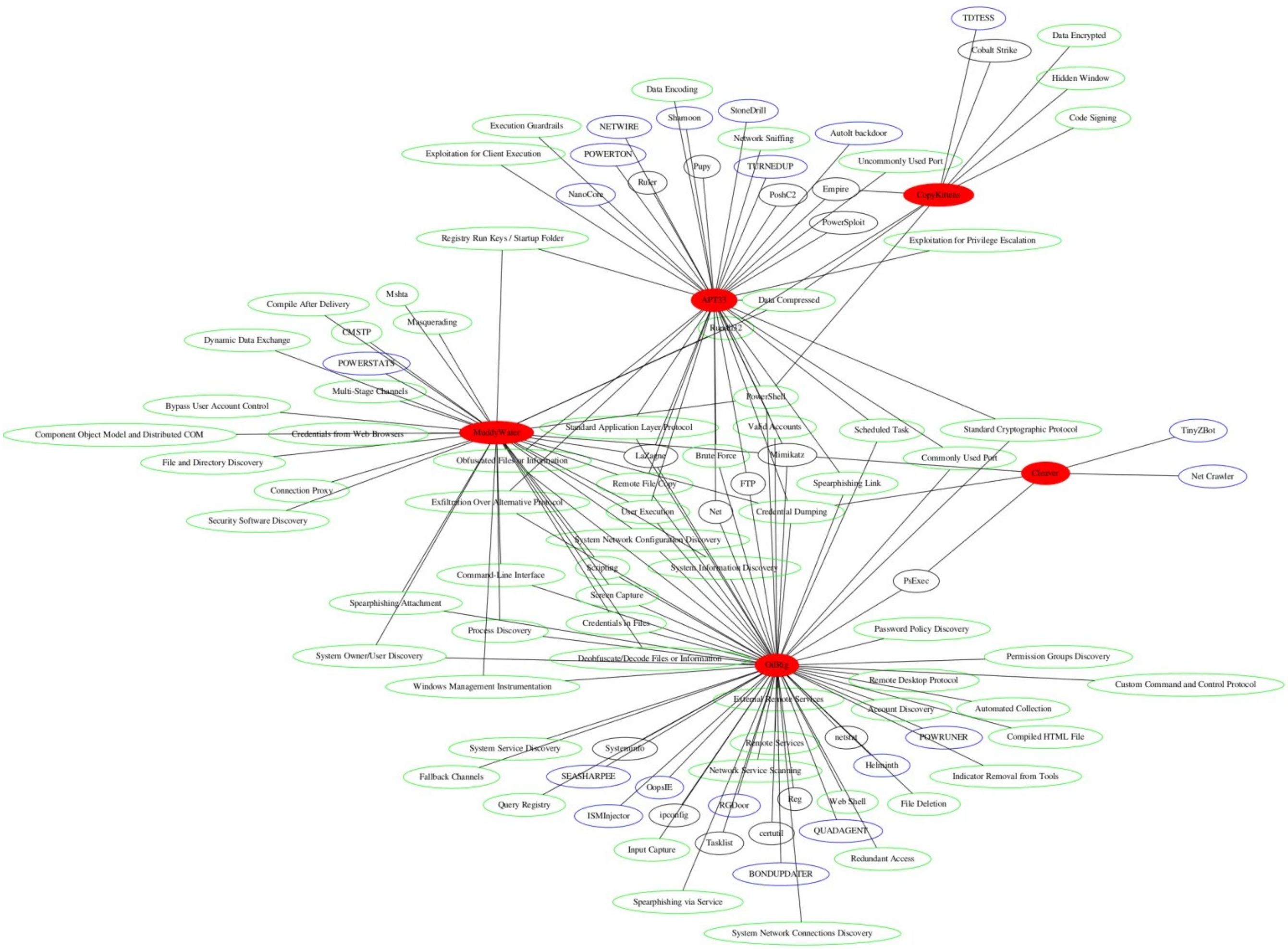
Cleaver TTP

Just like **Charming Kitten** (*which is not included into this report since it is a quite ongoing mistery even if a **great** report from **Clear Sky** is available*), Cleaver is a threat group that is responsible of **one** of the first most advanced and silent cyber attack attributed to Iran known until now (**OpCleaver**, by Cylance). Cleaver attack capabilities are evolved over time very quickly and, according to Cylance, active since 2012. They look like to have infiltrated some of the world economic powers (ref: **here**) such as: Canada, China, England, France, Germany, India, Israel, Kuwait, Mexico, Pakistan, Qatar, Saudi Arabia, South Korea, Turkey, United Arab Emirates, and the United States. In the very first page of the OpCleaver report, the author writes that Cleaver is one of the most advanced threat actors ever. Even if I might agree with Cylance, I personally do not have such evidences so far, so I personally cannot compare Cleaver threat actor to the previus ones.

Threat Actors Comparison

Here comes the fun ! How about taking all these graphs and compare them ? Common references would highlight similarities, scopes and common TTPs and fortunately we might appreciate them in the following unique network diagram. You might spend over 20 minutes to check details on the following graph and I might decide to write an essay over it, but I will not do it :D, I'd like focus on few but important thoughts.

The **iper-connection between** the analyzed groups (take a look to the following graph) could prove that those teams are really linked together. They share Techniques, Procedures, Tools and Infection Artifacts and everything we might observe looks like belonging with a unique **meta-actor**. We might agree that the **meta-actor** would be linked



Threat Actor Comparison

OilRig and APT33 are the most known groups attributed to Iran, they share many tools but they clearly have two different intent and two different code bases (writing about Malware). CopyKittens, for example, have been clustered more closed to APT33 while Muddywater looks like clustered straight at the middle of them. But if we closely analyze the purposes and the used Malware we might agree in aggregating Muddy close to APT33, actually the weight of shared code should be heavier compared to common tools or common techniques, but I did not represent such a detail into graphs.

However two different 'code experience' are observed. The first one mostly focused on scriptting (node, python, autoIT) which could underline a group of people evolving from IT department and later-on acquiring cyersecurity skills, while the second observed behavior is mostly oriented on deep development skills such as for example: Java, .NET and C++. On MuddyWater and APT33 side, the usage of scripting engines, the usage of powershell, and the usage of Empire framework tighten together, plus the lack of exploiting capabilities skills and looks to be mostly focused on stealth operations.

Conclusion

In this post I wrote a preliminary and personal analysis of threat actors attributed by the community to Iran, comparing TTPs coming from MITRE and relations extracted from Malpedia. The outcome is a proposal to consider the numerous groups (OilRig, APT33, MuddyWater, Cleaver, etc..) as a primary meta-threat-actor and dividing them by operations rather real group.

SHARE THIS:

Like this:

Like

Be the first to like this.

Posted in **apt**, **cybersecurity**, **experience**
Tagged **apt**, **CyberSecurity**, **muddywater**, **oilrig**, **Research**

PUBLISHED BY
marcoramilli

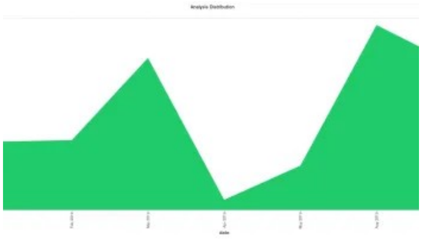
Ethical Hacking, Advanced Targeted Attack Expert and Malware Evasion Expert View all posts by marcoramilli

Related

OilRig: the techniques evolution over time

AUGUST 7, 2019

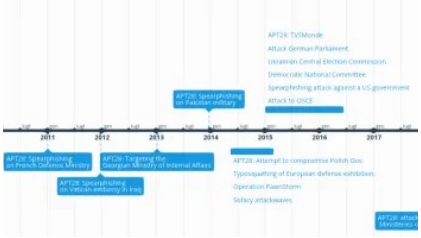
IN "APT"



After 1 Million of Analyzed Samples

NOVEMBER 25, 2019

IN "CYBERSECURITY"



APT28 Attacks Evolution

DECEMBER 5, 2019

IN "APT"

APT28 Attacks Evolution