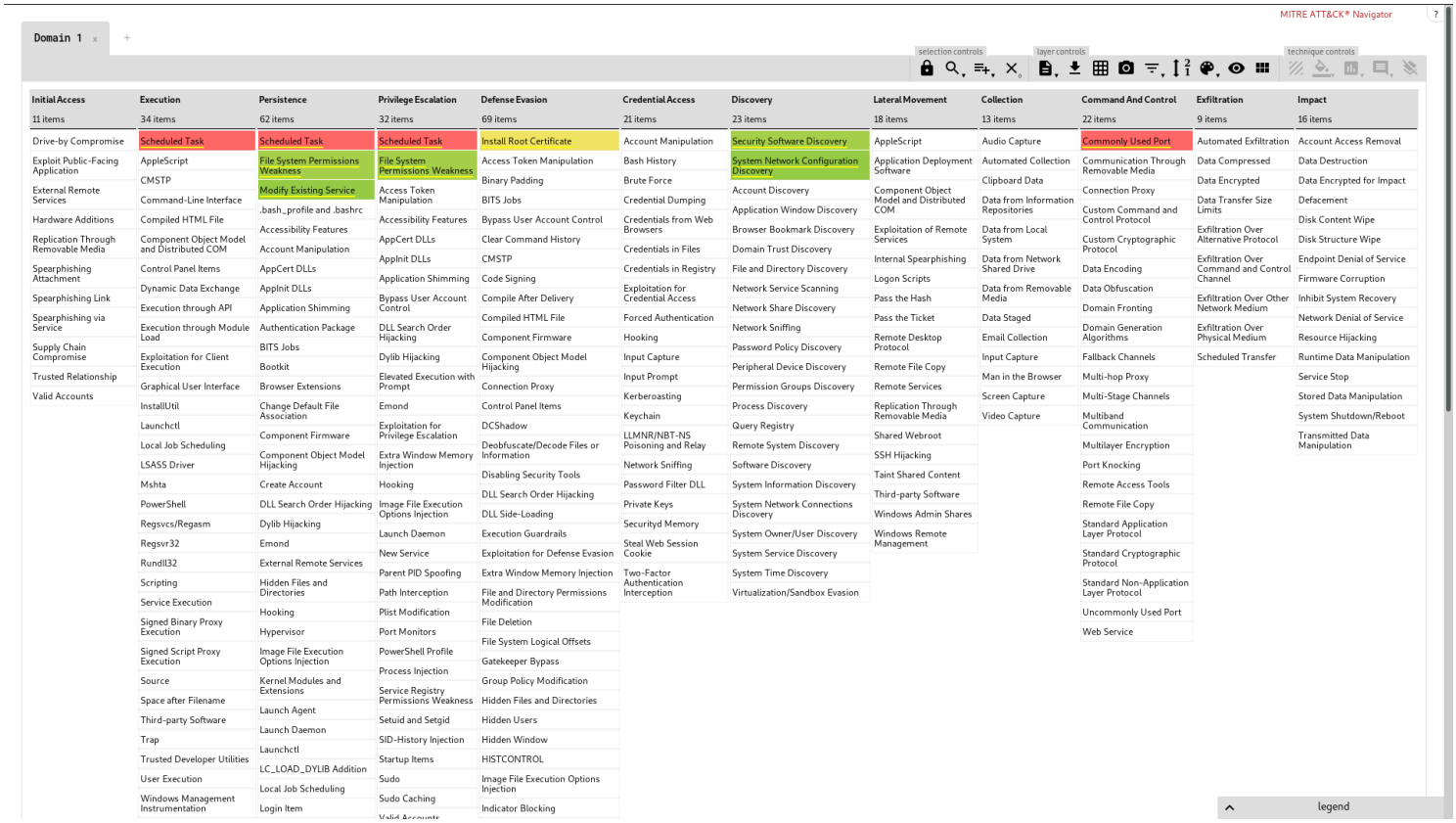
report.md

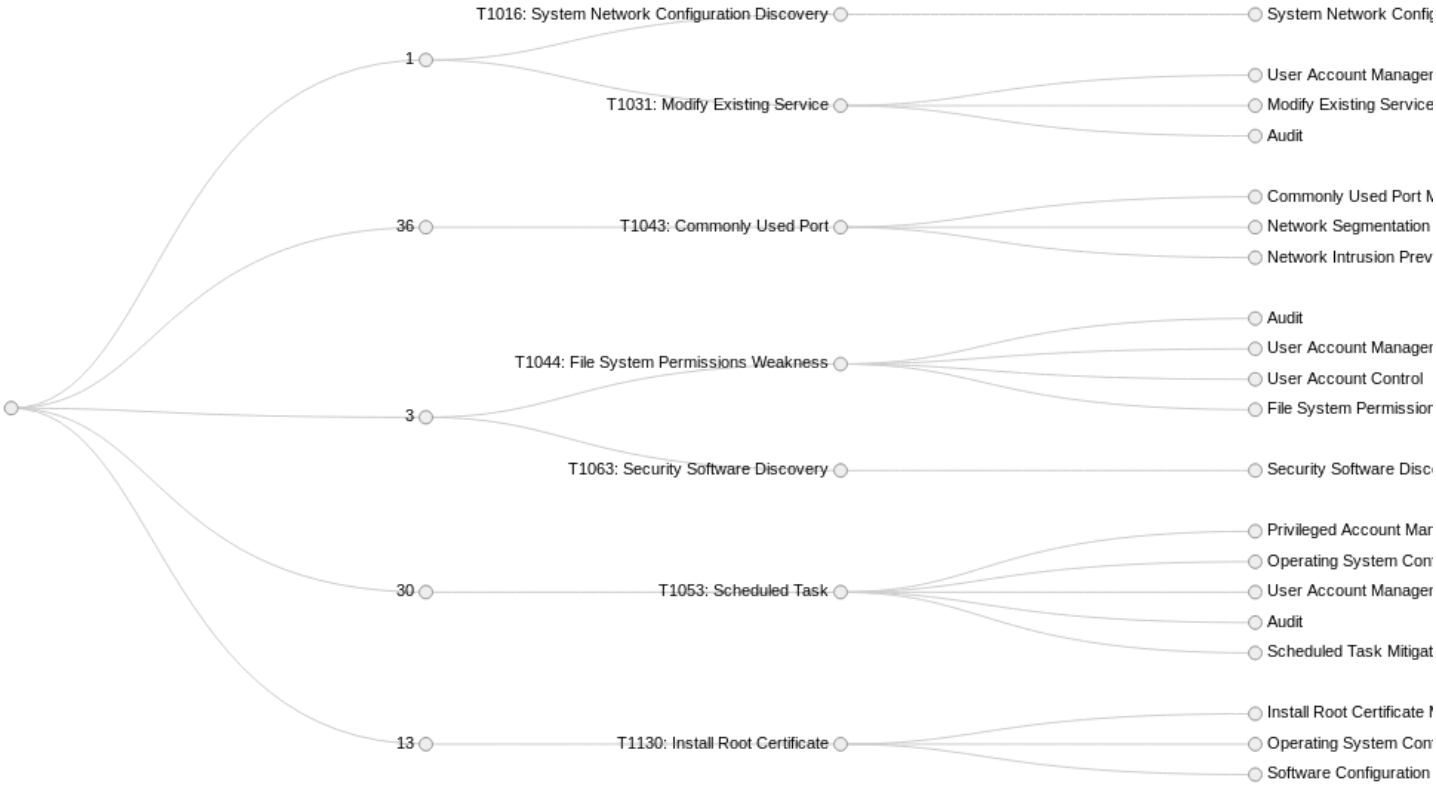
XS 2020 Report

> This report summarises techniques used by Red Team against [Domain 1]. The first part consists of graphs representing technique, mitigations and data sources for monitoring technique occurrence. There is a brief description of each adversary technique used against this domain, an example of atomic tests which can validate of implementation of monitoring/alerting tools, proposed mitigations and data sources necessary for monitoring. It is recommended to use this report along with five timestamps method for feedback purposes.

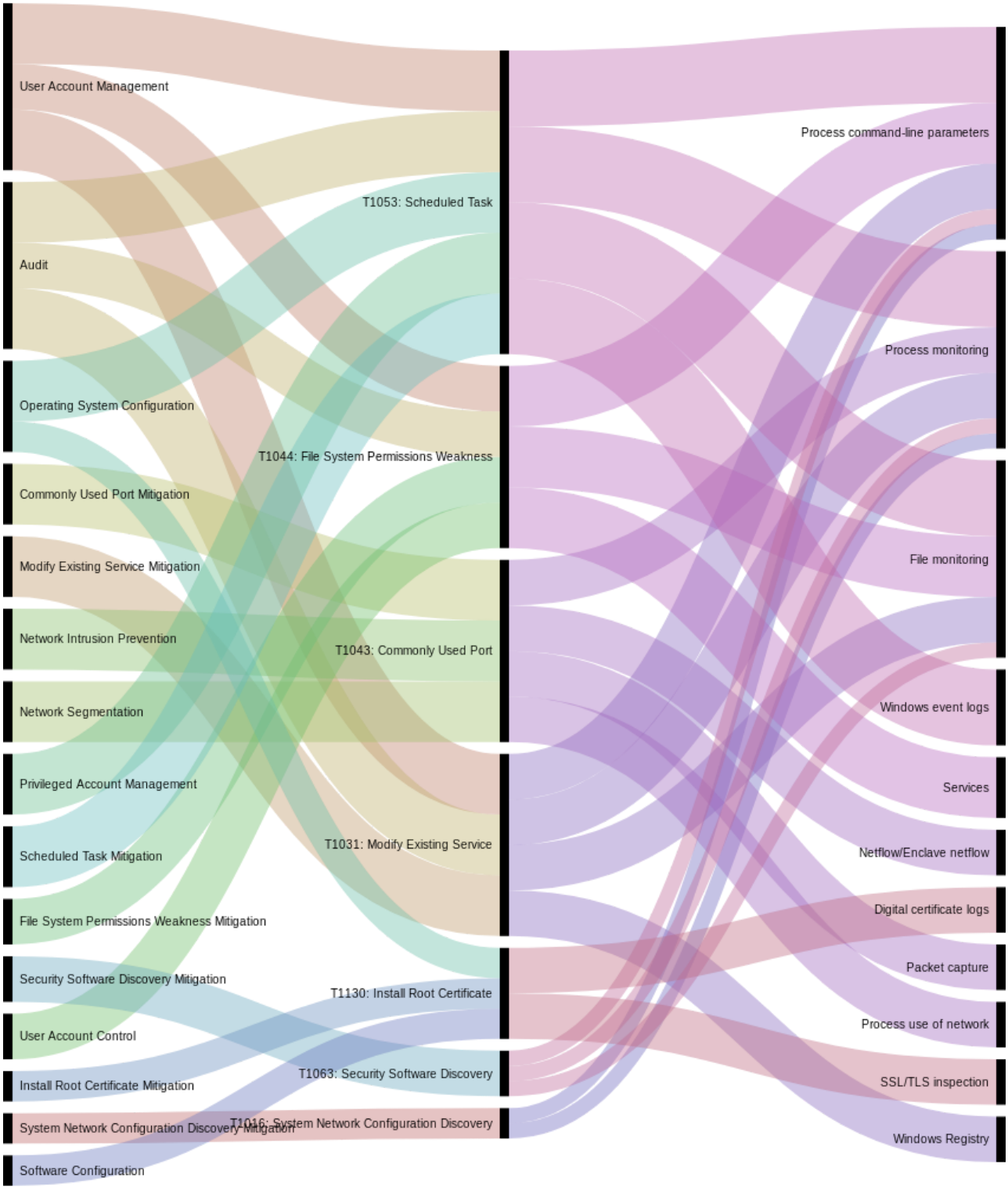
Graph 1: Used techniques visualised in ATT&CK matrix



Graph 2: Used techniques and their mitigations based on technique occurance

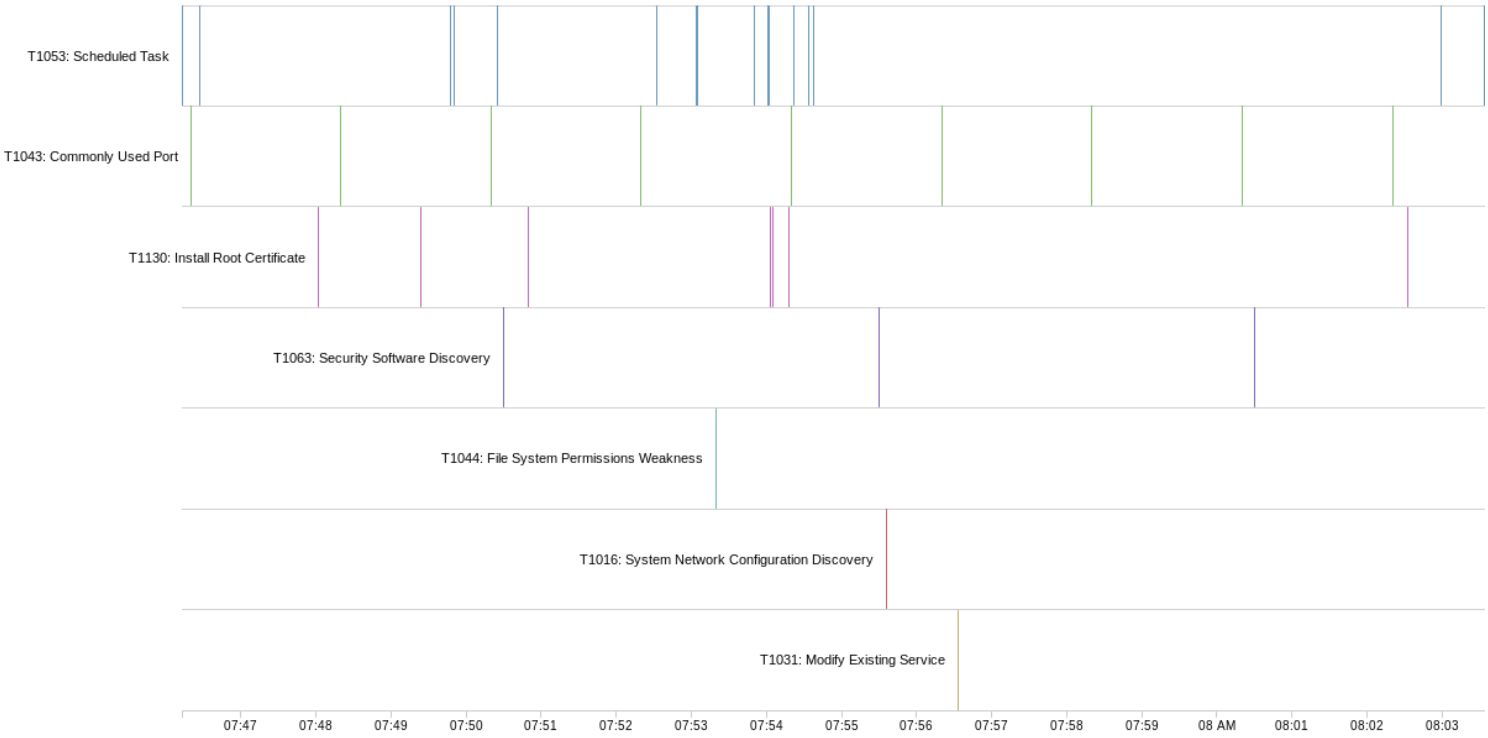


Graph 3: Mitigations, used techniques and sources for monitoring based on technique occurance



Graph 4: Used techniques and data sources for monitoring, based on technique occurance

Graph 5: Used techniques in time



Used techniques sorted by descending occurrance

- T1031: Modify Existing Service

T1031: Modify Existing Service

Description from ATT&CK

> Windows service configuration information, including the file path to the service's executable or recovery programs/commands, is stored in the Registry. Service configurations can be modified using utilities such as sc.exe and [Reg] (https://attack.mitre.org/software/S0075).
> Adversaries can modify an existing service to persist malware on a system by using system utilities or by using custom tools to interact with the Windows API. Use of existing services is a type of Masquerading that may make detection analysis more challenging. Modifying existing services may interrupt their functionality or may enable services that are disabled or otherwise not commonly used.
>
> Adversaries may also intentionally corrupt or kill services to execute malicious recovery programs/commands. (Citation: Twitter Service Recovery Nov 2017) (Citation: Microsoft Service Recovery Feb 2013)

Atomic Tests

- Atomic Test #1 - Modify Fax service to run PowerShell

Atomic Test #1 - Modify Fax service to run PowerShell

This test will temporarily modify the service Fax by changing the binPath to PowerShell and will then revert the binPath change, restoring Fax to its original state.

Upon successful execution, cmd will modify the binpath for `Fax` to spawn powershell. Powershell will then spawn.

Supported Platforms: Windows

Attack Commands: Run with `command_prompt` ! Elevation Required (e.g. root or admin)

```
sc config Fax binPath= "C:\windows\system32\WindowsPowerShell\v1.0\powershell.exe -noexit -c \"write-host 'T1031 Test'
sc start Fax
```

Cleanup Commands:

```
sc config Fax binPath= "C:\WINDOWS\system32\fxssvc.exe" >nul 2>&1
```

Mitigations for T1031:

User Account Management

Manage the creation, modification, use, and permissions associated to user accounts.

References

- mitre-attack:: https://attack.mitre.org/mitigations/M1018

Modify Existing Service Mitigation

Use auditing tools capable of detecting privilege and service abuse opportunities on systems within an enterprise and correct them. Limit privileges of user accounts and groups so that only authorized administrators can interact with service changes and service configurations. Toolkits like the PowerSploit framework contain the PowerUp modules that can be used to explore systems for Privilege Escalation weaknesses. (Citation: Powersploit)

Identify and block potentially malicious software that may be executed through service abuse by using whitelisting (Citation: Beechey 2010) tools like AppLocker (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) that are capable of auditing and/or blocking unknown programs.

References

- mitre-attack:: https://attack.mitre.org/mitigations/T1031
- Powersploit::PowerSploit. (n.d.). Retrieved December 4, 2014.

https://github.com/mattifestation/PowerSploit

- Beechey 2010::Beechey, J. (2010, December). Application Whitelisting: Panacea or Propaganda?. Retrieved November 18, 2014.

http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599

- Windows Commands JPCERT::Tomonaga, S. (2016, January 26). Windows Commands Abused by Attackers. Retrieved February 2, 2016.

http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html

- NSA MS AppLocker::NSA Information Assurance Directorate. (2014, August). Application Whitelisting Using Microsoft AppLocker. Retrieved March 31, 2016.

https://www.iad.gov/iad/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm

Audit

Perform audits or scans of systems, permissions, insecure software, insecure configurations, etc. to identify potential weaknesses.

References

- mitre-attack:: https://attack.mitre.org/mitigations/M1047

Detection of T1031:

Look for changes to service Registry entries that do not correlate with known software, patch cycles, etc. Changes to the binary path and the service startup type changed from manual or disabled to automatic, if it does not typically do so, may be suspicious. Tools such as Sysinternals Autoruns may also be used to detect system service changes that could be attempts at persistence. (Citation: TechNet Autoruns)

Service information is stored in the Registry at `HKLM\SYSTEM\CurrentControlSet\Services`.

Command-line invocation of tools capable of modifying services may be unusual, depending on how systems are typically used in a particular environment. Collect service utility execution and service binary path arguments used for analysis. Service binary paths may even be changed to execute cmd commands or scripts.

Look for abnormal process call trees from known services and for execution of other commands that could relate to Discovery or other adversary techniques. Services may also be modified through Windows system management tools such as Windows Management Instrumentation and PowerShell, so additional logging may need to be configured to gather the appropriate data.

Data Sources for T1031:

Windows Registry

File monitoring

Process monitoring

Process command-line parameters