

The Advanced Persistent Threat

A Cyber Security Challenge

Objectives

- What is Advanced Persistent Threat (APT)
- APT characteristics
- APT challenges
- APT examples
- Symptoms of an organisation being targeted by an APT
- Intrusion detection techniques
- A correlation-based system for real-time APT detection and prediction

What Is Advanced Persistent Threat (APT)

- Well-funded, organised attack groups that have interest in data theft
- A cybercrime category directed at business and political targets
 - Advanced
 - Persistent
 - Threat

APT Life Cycle



Social Engineering Attack

Preparing the ground for the attack:

- Identifying the victim(s).
- Gathering background information.
- Selecting attack method(s).

Closing the interaction, ideally without arousing suspicion:

- Removing all traces of malware.
- Covering tracks.
- Bringing the charade to a natural end.



Deceiving the victim(s) to gain a foothold:

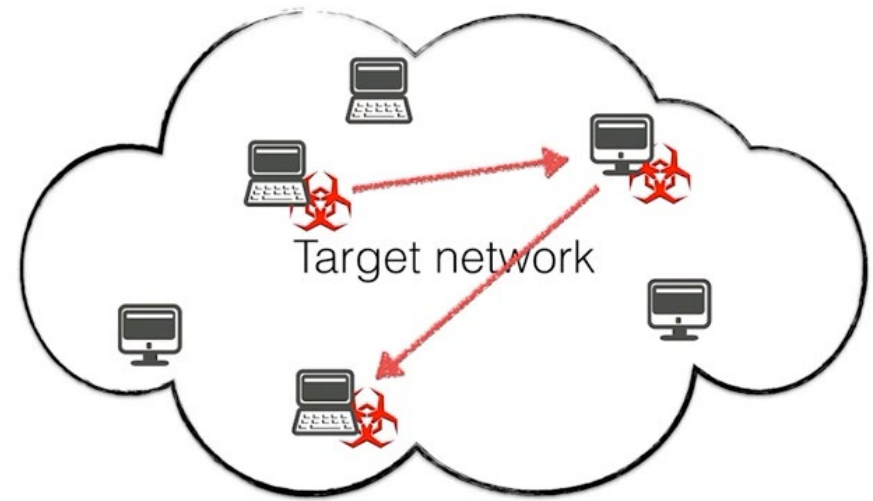
- Engaging the target.
- Spinning a story.
- Taking control of the interaction.

Obtaining the information over a period of time:

- Expanding foothold.
- Executing the attack.
- Disrupting business or/and siphoning data.

APT Characteristics

- APTs are motivated by long-term goals aiming at espionage and political manoeuvring
- Make use of multiple attack vectors and tools
- High degree of stealthiness
- Data exfiltration



APT Challenges

- APTs are targeting selected organizations
- The economic damage resulting of a successful APT can be very expensive
- APTs form a problem for the current detection methods

APT Examples

- The GhostNet cyberespionage operation
 - Was discovered in 2009, executed from China
 - The attackers focused on gaining access to the network devices of government ministries and embassies
- The Stuxnet worm
 - Used to attack Iran's nuclear program, detected in 2010
 - The malware targeted SCADA (Supervisory Control and Data Acquisition) systems

APT Examples

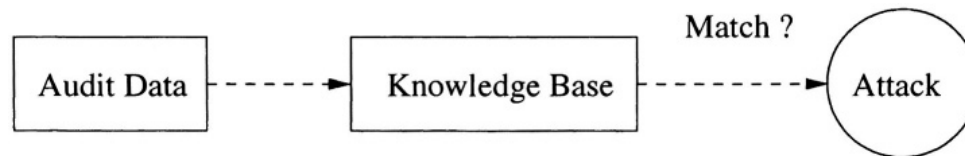
- APT28, the Russian advanced persistent threat group also known as Cozy Bear
 - Has been linked to a number of attacks, including a 2015 spear phishing attack on the Pentagon, as well as the 2016 attacks on the Democratic National Committee
- APT34, an advanced persistent threat group linked to Iran
 - Was identified in 2017 by researchers at FireEye, but has been active since at least 2014
 - The threat group has targeted companies in the Middle East with attacks against financial, government, energy, chemical and telecommunications companies
- APT37, also known as Reaper, StarCruft and Group 123
 - An advanced persistent threat linked to North Korea that is believed to have originated around 2012
 - APT37 has been connected to spear phishing attacks exploiting an Adobe Flash zero-day vulnerability

Symptoms of an Organisation Being Targeted by an APT

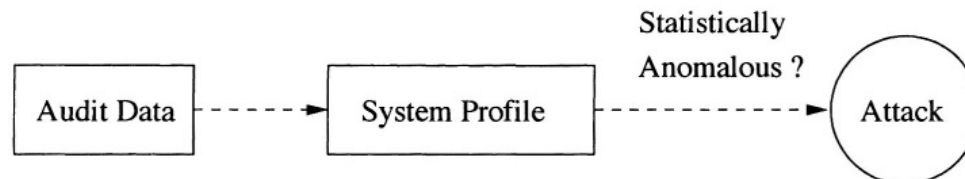
- Unusual activity on user accounts
- Extensive use of backdoor Trojan horse malware
- Odd or uncharacteristic database activity
- Presence of unusual data files

Intrusion Detection Techniques

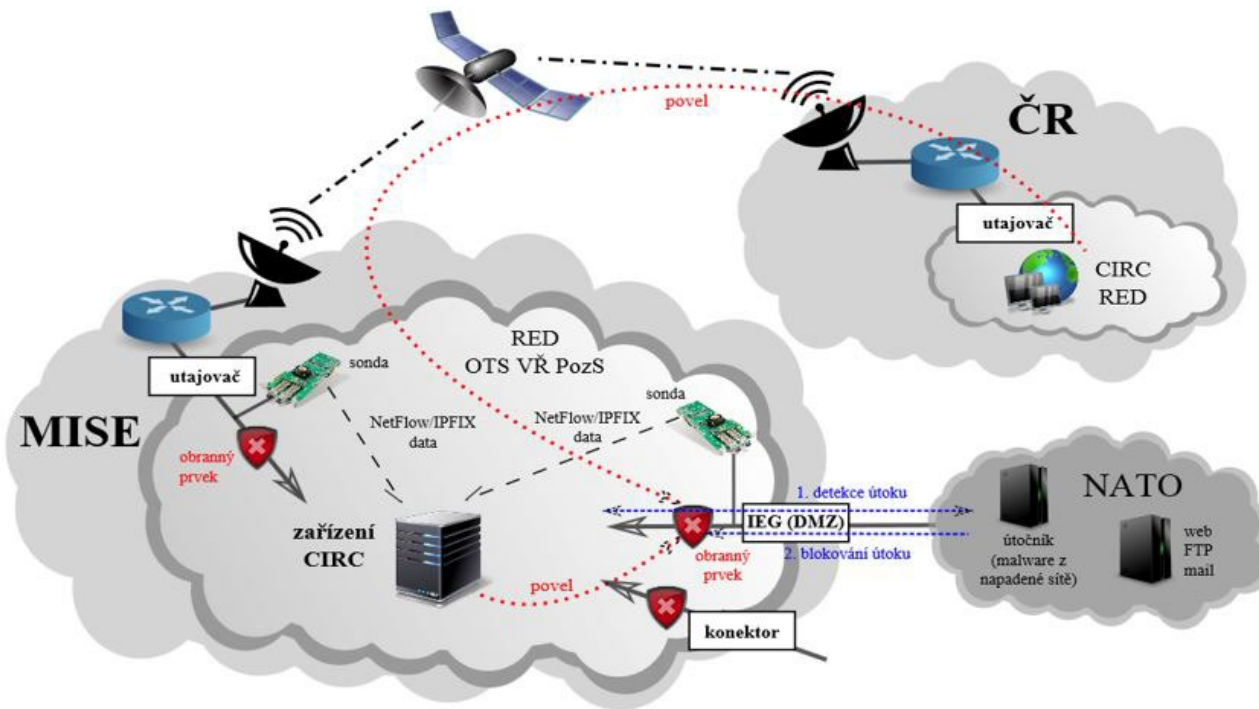
- Static techniques
 - Depend on investigating the hosts' logs after the attack has occurred
- Dynamic techniques
 - Signature-based



- Anomaly-based



A Correlation-based System for Real-time APT Detection and Prediction

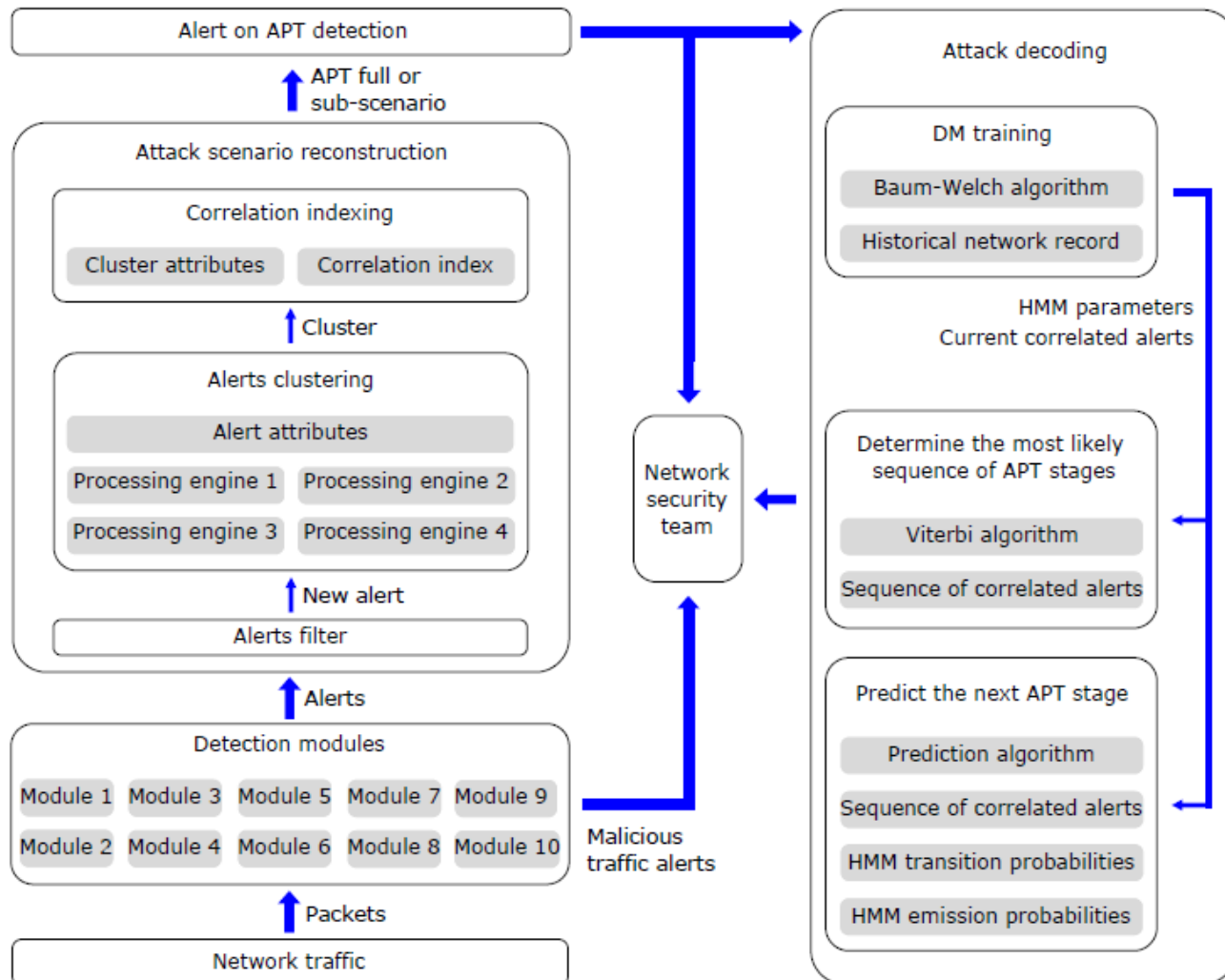


A Correlation-based System for Real-time APT Detection and Prediction

Acknowledgement:

- The developed detection modules of this work were supported by the project CYBER-2, funded by the Ministry of Defence of the Czech Republic under contract No. 1201 4 7110
- The developed detection and prediction frameworks were supported in part by the Gulf Science, Innovation and Knowledge Economy Programme of the U.K. Government under UK-Gulf Institutional Link Grant IL 279339985 and in part by the Engineering and Physical Sciences Research Council (EPSRC), U.K., under Grant EP/R006385/1
 - I. Ghafir, K. G. Kyriakopoulos, S. Lambotharan, F. J. Aparicio-Navarro, B. Assadhan and H. Binsalleeh, "Hidden Markov Models and Alert Correlations for the Prediction of Advanced Persistent Threats," IEEE Access (IF=4.098), vol. 7, pp. 99508-99520, 2019
<https://ieeexplore.ieee.org/document/8767917>

A Correlation-based System for Real-time APT Detection and Prediction

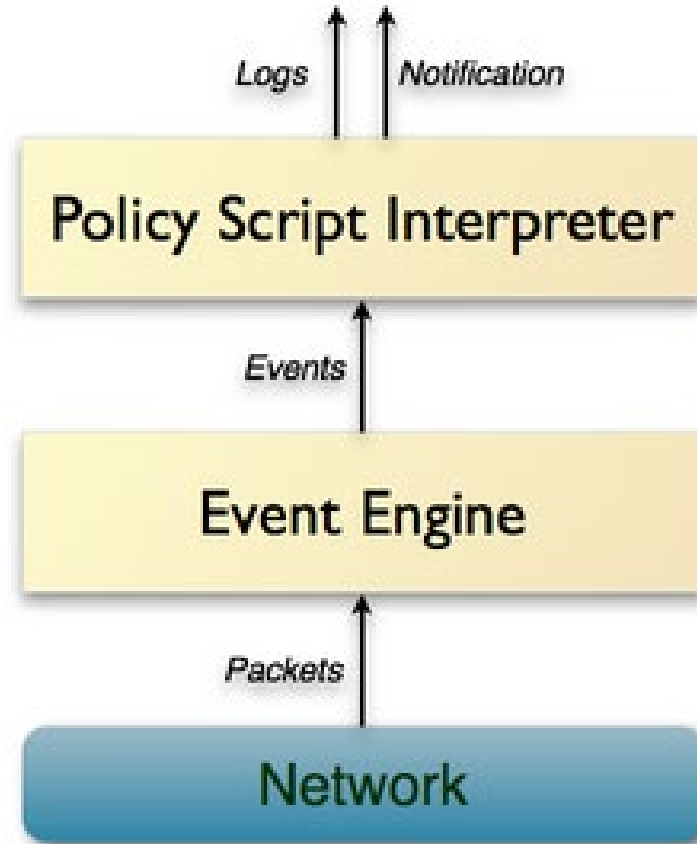


Detection Modules

- Disguised exe file detection
- Malicious file hash detection
- Malicious domain name detection
- C&C communication detection
- Malicious SSL certificate detection
- Domain flux detection
- Scan detection
- TOR connection detection

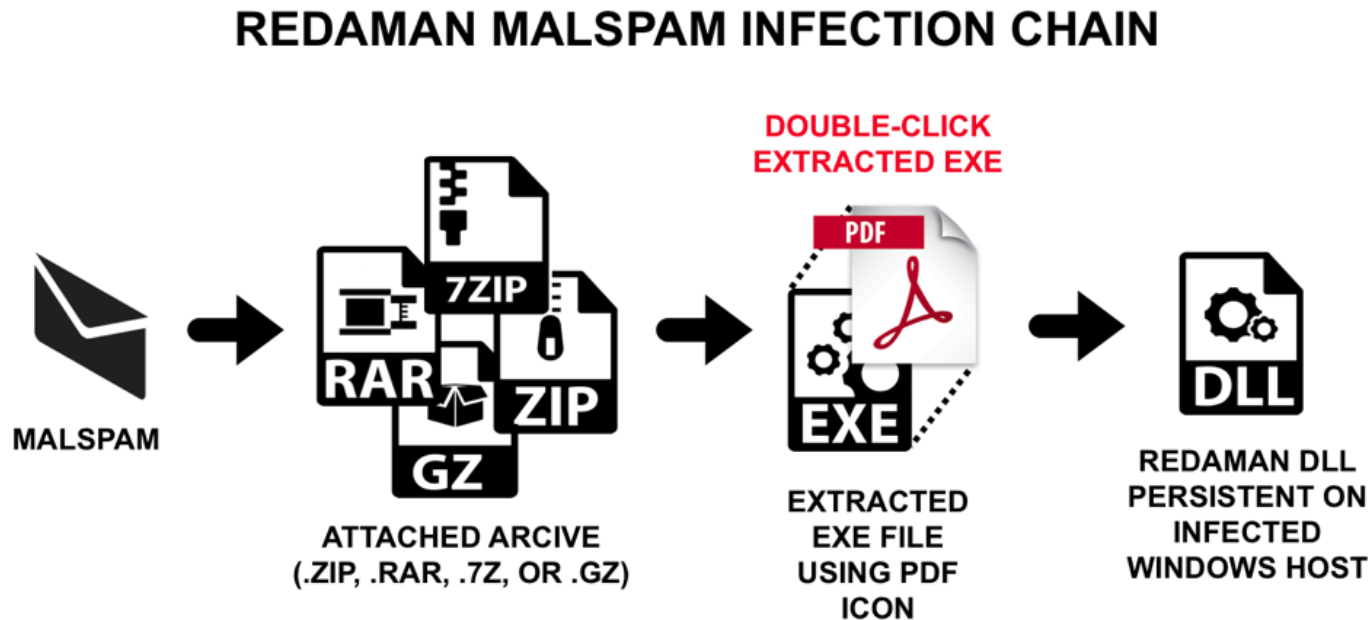


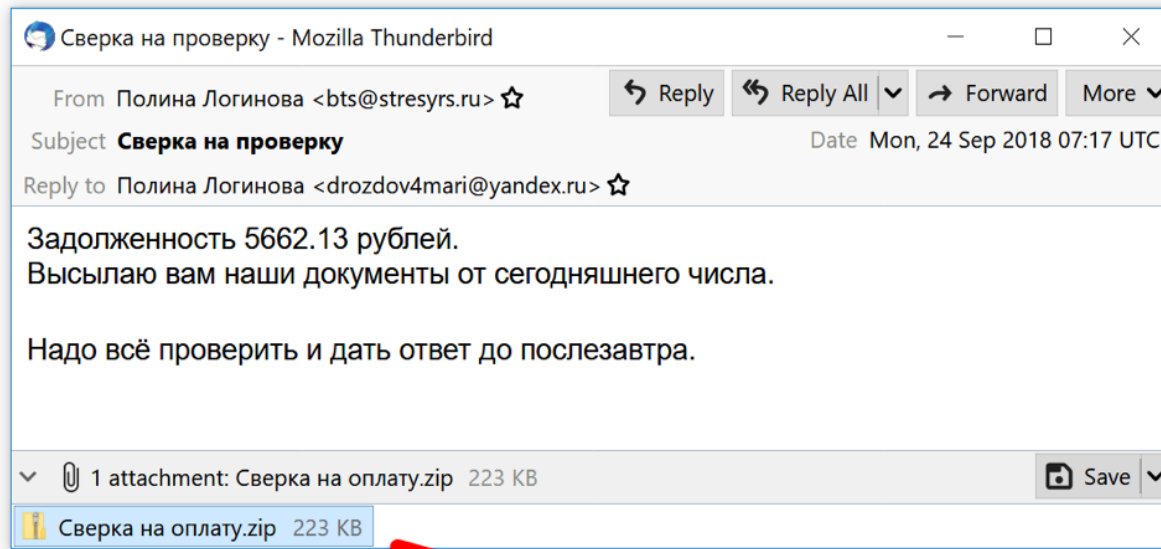
The Zeek Network Security Monitor



Disguised exe File Detection (DeFD)

- The attacker changes the original extension of a piece of malware
- Redaman banking malware





Capabilities of Redaman:

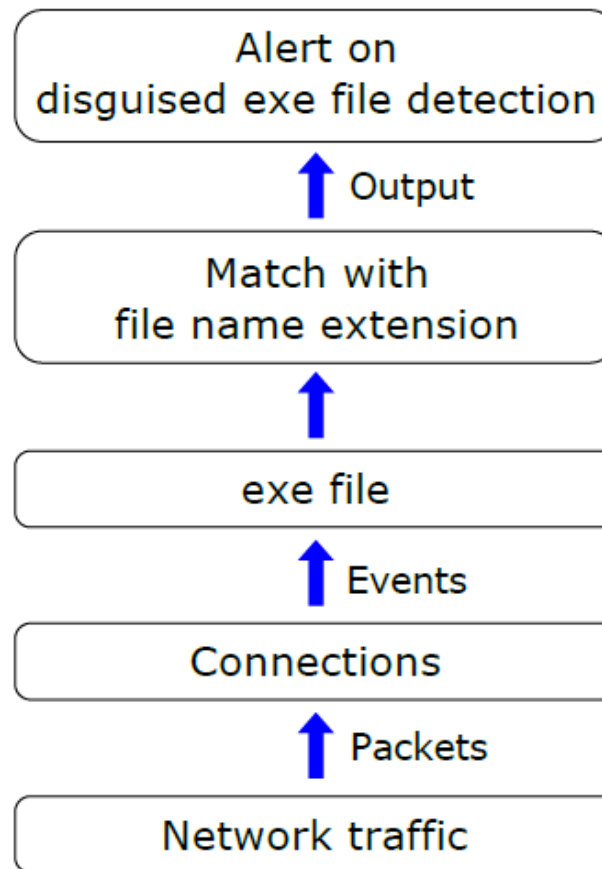
- Monitoring browser activity
- Downloading files to the infected host
- Keylogging activity
- Capture screen shots
- Collecting and exfiltrating financial data
- Shutting down the infected host
- Altering DNS configuration through the Windows host file
- Retrieving clipboard data
- Adding certificates to the Windows store

Disguised exe File Detection (DeFD)

Algorithm 1 Implementation pseudo-code of DeFD

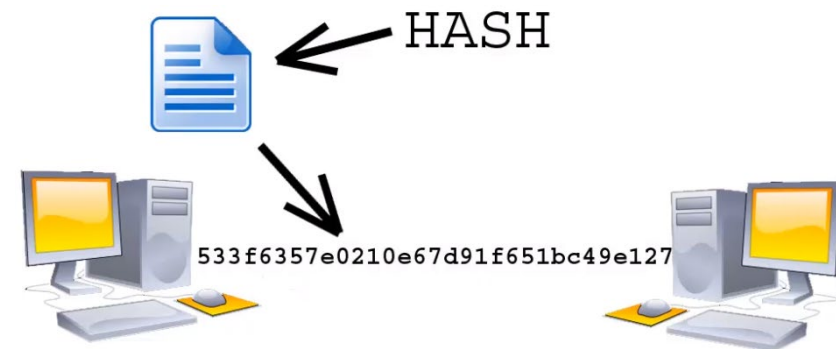
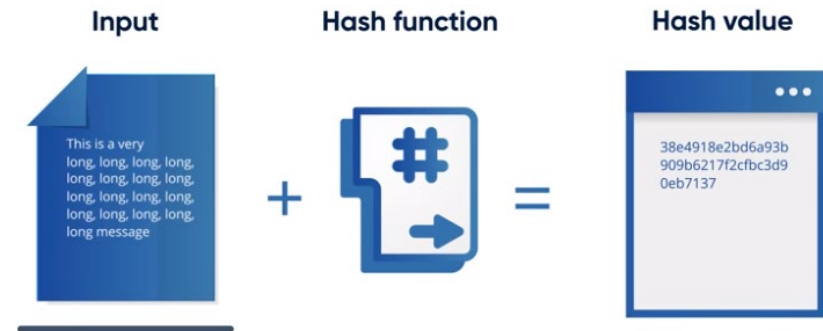
```
1: Get t_exe_file table
2: Get file_over_new_connection event
3: fname  $\leftarrow$  file name
4: if the connection is established by a host from the monitored
5:   network then
6:   | if the file MIME type is in t_exe_file table then
7:   | | if file MIME type = fname extension then
8:   | | | if the same disguised_exe_alert has been generated over
9:   | | |   the last day then
10:  | | |   goto End
11:  | | | else
12:  | |   Generate an event (disguised_exe_alert)
13:  | |   Write disguised_exe_alert into disguised_exe_detection.log
14:  | |   Send an alert email to RT
15:  | |   Suppress the same disguised_exe_alert over the next day
16:  | | end if
17:  | | else
18:  |   goto End
19:  | end if
20:  else
21:  | goto End
22:  end if
23: else
24:   goto End
25: end if
26: End
```

Disguised exe File Detection (DeFD)



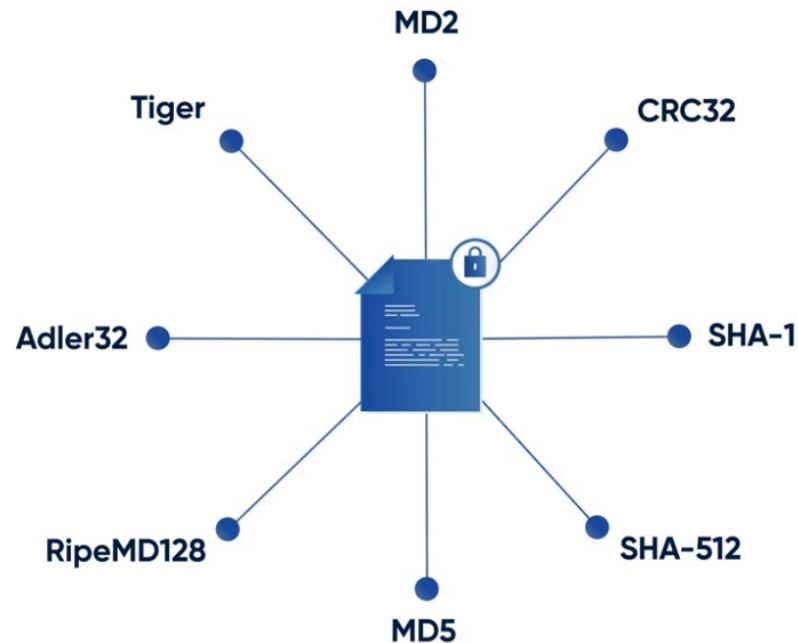
Malicious File Hash Detection (MFHD)

- Hashing is an algorithm that calculates a fixed-size bit string value from a file
- Avalanche effect
- Unidirectional process
- Should be complex enough



Malicious File Hash Detection (MFHD)

- Used to compare two files for equality
- Used to verify the integrity

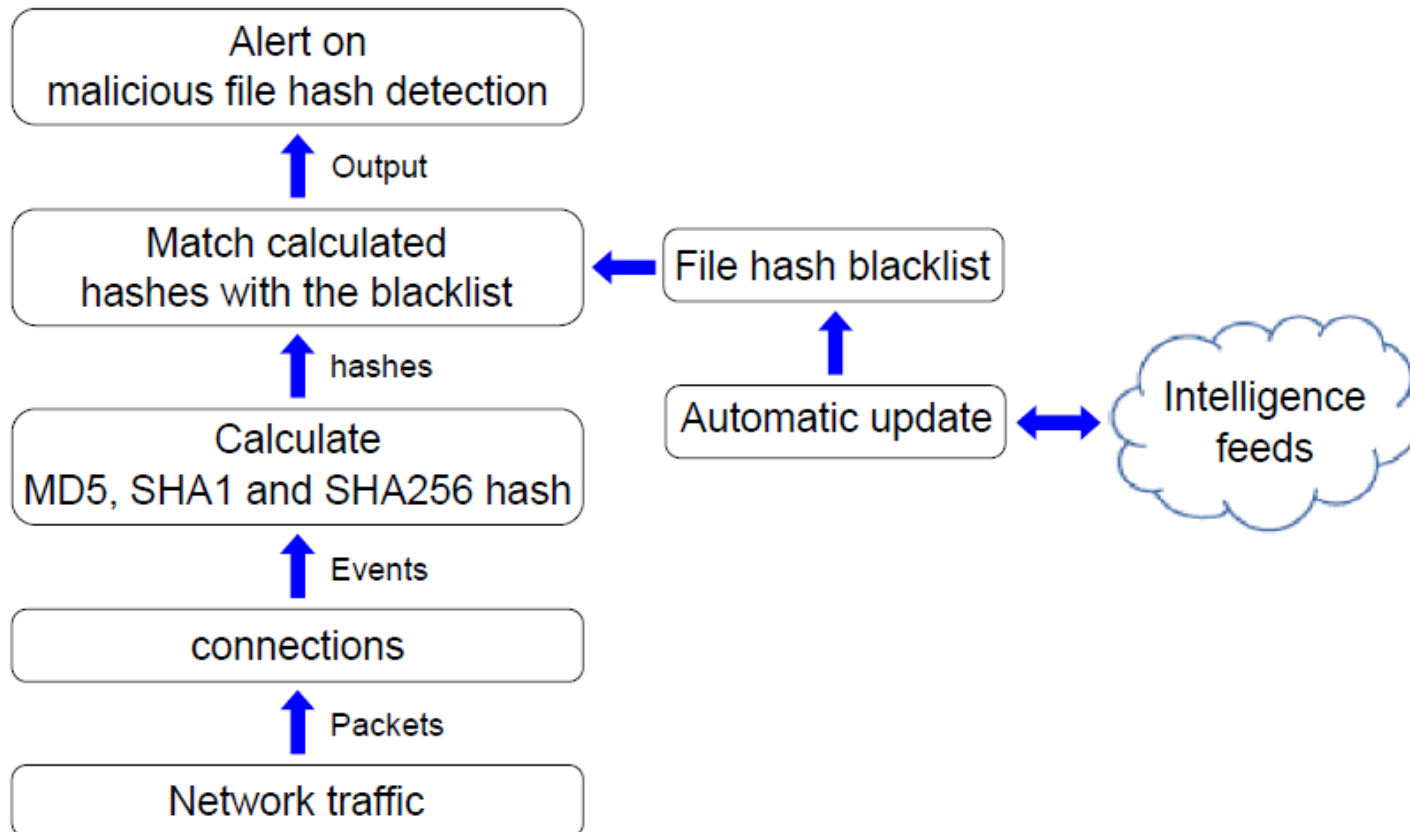


Malicious File Hash Detection (MFHD)

Algorithm 2 Implementation pseudo-code of MFHD

```
1: Get malicious fills hashes blacklist (blacklist.intel)
2: Get file_new event
3: Calculate MD5, SHA1 and SHA256 hashes
4: Send MD5, SHA1 and SHA256 hashes to Bro Intelligence Framework
5: if MD5, SHA1 or SHA256 hashes are in blacklist.intel then
6: |   if the connection is oriented to a host from the monitored
7: |       network then
8: | |   if the same hash_alert has been generated over the last
9: | |       day then
10: | |       goto End
11: | |   else
12: | |       Generate an event (hash_alert)
13: | |       Write hash_alert into blacklist_detection_hash.log
14: | |       Send an alert email to RT
15: | |       Suppress the same hash_alert over the next day
16: | |   end if
17: |   else
18: |       goto End
19: |   end if
20: else
21:     goto End
22: end if
23: End
```

Malicious File Hash Detection (MFHD)



Acknowledgement

This material uses resources from:

- I. Ghafir, K. G. Kyriakopoulos, S. Lambotharan, F. J. Aparicio-Navarro, B. Assadhan, H. Binsalleeh and Diab M. Diab, “Hidden Markov Models and Alert Correlations for the Prediction of Advanced Persistent Threats,” IEEE Access, 2019.
- I. Ghafir, M. Hammoudeh, V. Prenosil, L. Han and R. Hegarty, K. Rabie and F. J. Aparicio-Navarro, “Detection of Advanced Persistent Threat Using Machine-Learning Correlation Analysis,” Future Generation Computer Systems, vol. 89, pp. 349-359, 2018.
- Verma, R.M. and Marchette, D.J., 2019. Cybersecurity Analytics. CRC Press.
- Cyber Security Tutorial - Cyber Security Training For Beginners. Simplilearn.
- Humayun, M., Niazi, M., Jhanjhi, N.Z., Alshayeb, M. and Mahmood, S., 2020. Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. Arabian Journal for Science and Engineering, pp.1-19.
- Madarie, R., 2017. Hackers' Motivations: Testing Schwartz's Theory of Motivational Types of Values in a Sample of Hackers. International Journal of Cyber Criminology, 11(1).
- Akbanov, M., Vassilakis, V.G. and Logothetis, M.D., 2019. WannaCry ransomware: Analysis of infection, persistence, recovery prevention and propagation mechanisms. Journal of Telecommunications and Information Technology.