Network Attacks Insight/Overview

Simona Buchovecká, Tomáš Čejka

Faculty of Information Technology, CTU in Prague

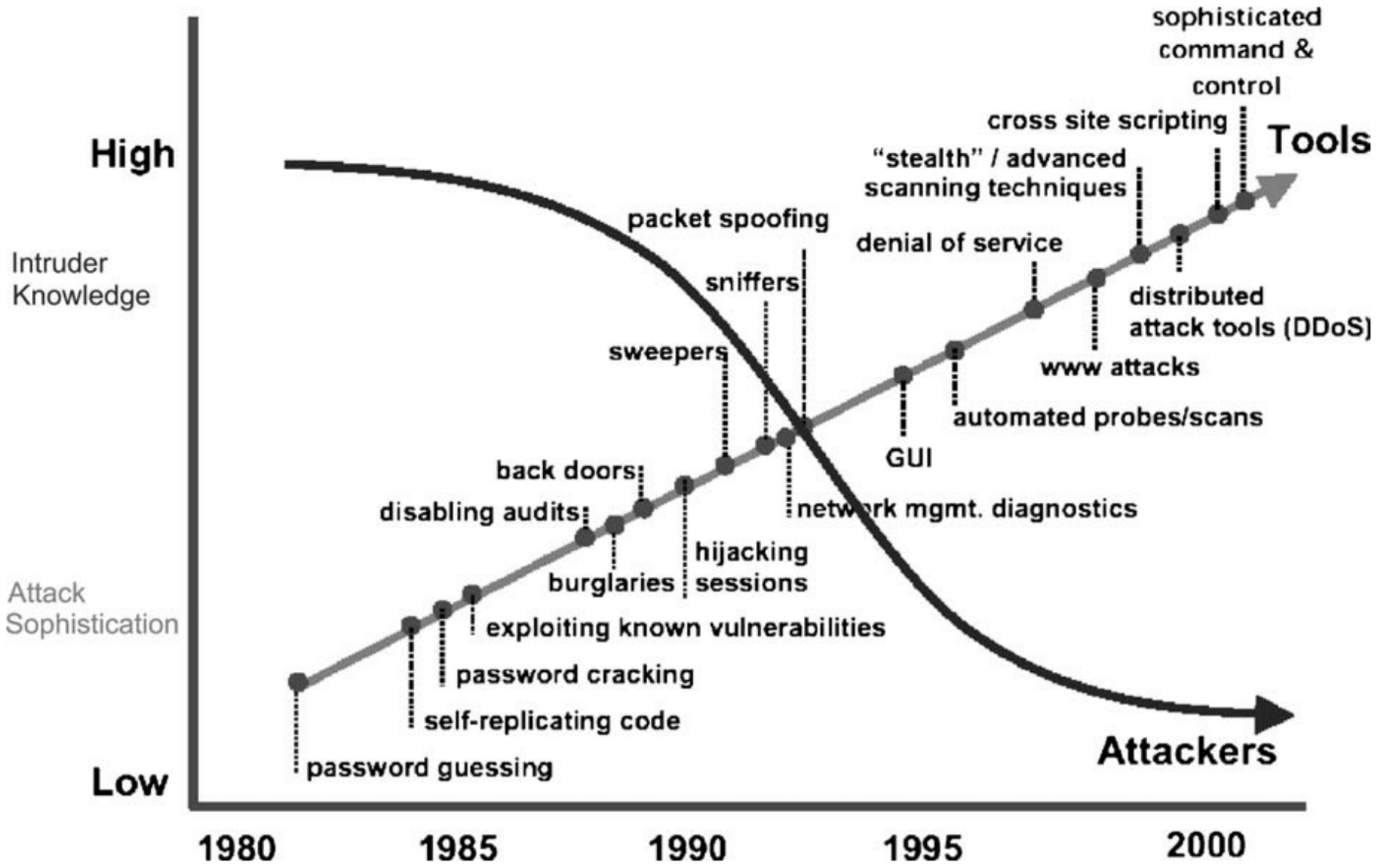
simona.buchovecka@fit.cvut.cz, tomas.cejka@fit.cvut.cz

February 21, 2021

Section 1

Evolution

History of Attacks



Present, Discussion

- Ransomware
- Wireless attacks (KRACK)
- IoT botnets (Mirai)
- Philips hue
- Cryptominers
- Hardware attacks
  (CPU arch: Spectre, meltdown, cache attacks)
- “side-channel attacks”

Botnets

- Infected devices, synchronized, collaborating
- Different ways of communication:
  - Central Command&Control (C&C / C2) servers (channels: IRC, ICQ, HTTP, favicon, DNS)
  - P2P botnets
- Usually fastflux domains

Section 2

Classification

Attack Vector / Indicator of Compromise

Attack Vector describe how an attack can be performed and what it exploits.

Indicator of compromise in computer forensics is an artifact observed on a network or in an operating system that with high confidence indicates a computer intrusion.

Examples: Fragmented packets exploiting buffer overflow vulnerability in some particular software; packets with spoofed srcip with 123/UDP dstport sent to an NTP server.

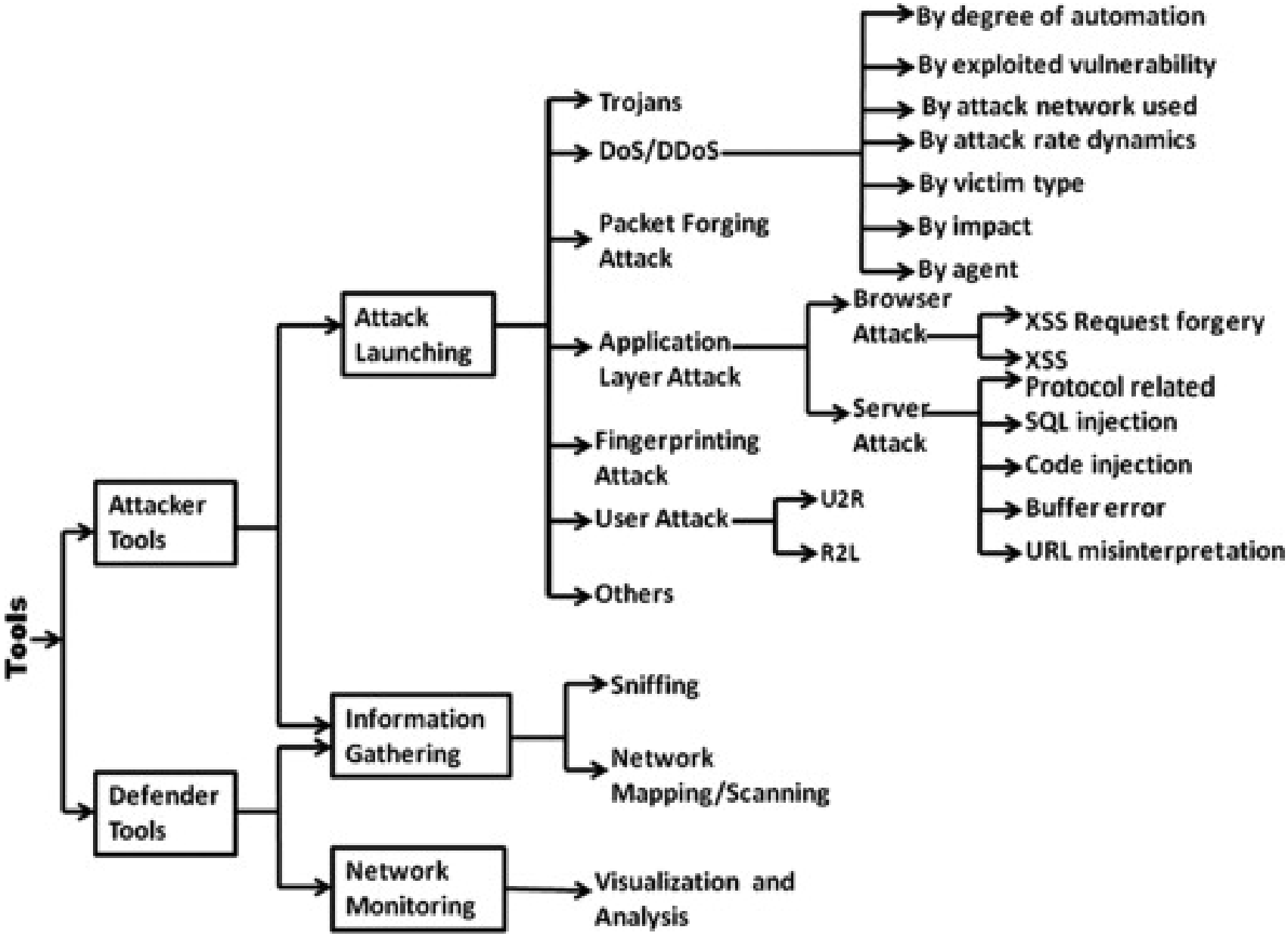
Ways of Classification

There are many different classification methodologies.
Hansman et al.: Based on dimensions:

- 1st dimension to categorise the attack based on attack vector,
- 2nd dimension based on attack targets,
- 3rd dimension covers vulnerabilities and exploits that attack uses,
- 4th dimension deals with attacks having payloads or effects beyond themselves,
- other dimensions can be added.

There are many taxonomies of attack techniques, e.g.,
`https://attack.mitre.org/` is popular.

Example of taxonomy



Brief List of Attack Types

- Information Gathering:
  - Scanning (vertical/horizontal)
  - OSINT (Open Source Intelligence), *INT
- Credential Stealing
  - Phishing
  - Brute-force attacks (dictionary attacks)
- Communication intercept
  - Man-in-the-Middle
  - Poisoning
  - Hijacking
- Service/operation disruption
  - (D)DoS
  - Starvation
  - De-authentication/Connection resetting
- Data Exfiltration
  - Covert Channels
  - Tunnels / VPNs

Section 3

Related Topics

Forms of Protection

- Access Control
- Authentication
- Confidentiality
- Integrity
- Non-repudiation

Sources of Security Threats

- Design Philosophy
- Weaknesses in Network Infrastructure and Communication Protocols
- Rapid Growth of Cyberspace
- The Growth of the Hacker Community
- Vulnerability in Operating System Protocol
- The Invisible Security Threat: The Insider Effect
- Social Engineering
- Physical Theft

Security Threat Motives

- Terrorism
- Military Espionage
- Economic Espionage
- Targeting the National Information Infrastructure
- Vendetta/Revenge
- Hate (National Origin, Gender, and Race)
- Notoriety
- Greed
- Ignorance

Section 4

Observation & Monitoring

Attack Observation via Monitoring

General Classification

- Host-Based (system logs, auditing tools, . . .)
- Network-Based

Interaction in the network

- Active (`ping`, `iperf`, `traceroute`, Atlas RIPE, PerfSonar)
- Passive

Attack Observation via Monitoring

Monitoring data unit

- Counter
  - High-level information (total numbers of packets/bytes/errors, packet loss)
  - e.g. SNMP, Network Telemetry
- Packet
  - "Raw data"
  - Deep Packet Inspection (DPI)
  - Pattern matching
- Flow
  - high-level overview, communication of devices without full content
  - aggregation

IP Flow

An IP Flow, also called a Flow, is defined as a set of IP packets passing an Observation Point in the network during a certain time interval. All packets that belong to a particular Flow have a set of common properties derived from the data contained in the packet and from the packet treatment at the Observation Point.

(Cisco Systems NetFlow Services Export Version 9)

Classification of IP Flows

- uni-flow
  - unidirectional communication between srcip and dstip
- bi-flow
  - bidirectional
  - pairing flow records in time
  - advantage: requests and responses are matched before analysis

How Do Attacks Look Like?

Packet point of view

1	0.000000	172.16.0.8	64.13.134.52	TCP	58	36050	443	36050 → 443 [SYN] Seq=0 Win=3072 Len=0 MSS=1460
2	0.001539	172.16.0.8	64.13.134.52	TCP	58	36050	143	36050 → 143 [SYN] Seq=0 Win=3072 Len=0 MSS=1460
3	0.001597	172.16.0.8	64.13.134.52	TCP	58	36050	3306	36050 → 3306 [SYN] Seq=0 Win=2048 Len=0 MSS=1460
4	0.001650	172.16.0.8	64.13.134.52	TCP	58	36050	199	36050 → 199 [SYN] Seq=0 Win=3072 Len=0 MSS=1460
5	0.001703	172.16.0.8	64.13.134.52	TCP	58	36050	111	36050 → 111 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
6	0.001755	172.16.0.8	64.13.134.52	TCP	58	36050	1025	36050 → 1025 [SYN] Seq=0 Win=4096 Len=0 MSS=1460
7	0.001807	172.16.0.8	64.13.134.52	TCP	58	36050	995	36050 → 995 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
8	0.001861	172.16.0.8	64.13.134.52	TCP	58	36050	587	36050 → 587 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
9	0.001913	172.16.0.8	64.13.134.52	TCP	58	36050	53	36050 → 53 [SYN] Seq=0 Win=3072 Len=0 MSS=1460
10	0.001965	172.16.0.8	64.13.134.52	TCP	58	36050	5900	36050 → 5900 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
11	0.063797	64.13.134.52	172.16.0.8	TCP	60	53	36050	53 → 36050 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380
12	0.065271	172.16.0.8	64.13.134.52	TCP	58	36050	21	36050 → 21 [SYN] Seq=0 Win=4096 Len=0 MSS=1460
13	0.065341	172.16.0.8	64.13.134.52	TCP	58	36050	113	36050 → 113 [SYN] Seq=0 Win=4096 Len=0 MSS=1460
14	0.126832	64.13.134.52	172.16.0.8	TCP	60	113	36050	113 → 36050 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
15	0.129000	172.16.0.8	64.13.134.52	TCP	58	36050	80	36050 → 80 [SYN] Seq=0 Win=3072 Len=0 MSS=1460
16	0.129075	172.16.0.8	64.13.134.52	TCP	58	36050	139	36050 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
17	0.189975	64.13.134.52	172.16.0.8	TCP	60	80	36050	80 → 36050 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380
18	0.191518	172.16.0.8	64.13.134.52	TCP	58	36050	3389	36050 → 3389 [SYN] Seq=0 Win=3072 Len=0 MSS=1460
19	0.191589	172.16.0.8	64.13.134.52	TCP	58	36050	23	36050 → 23 [SYN] Seq=0 Win=2048 Len=0 MSS=1460
20	1.202878	172.16.0.8	64.13.134.52	TCP	58	36051	23	36051 → 23 [SYN] Seq=0 Win=2048 Len=0 MSS=1460
21	1.202974	172.16.0.8	64.13.134.52	TCP	58	36051	3389	36051 → 3389 [SYN] Seq=0 Win=2048 Len=0 MSS=1460
22	1.203041	172.16.0.8	64.13.134.52	TCP	58	36051	139	36051 → 139 [SYN] Seq=0 Win=4096 Len=0 MSS=1460
23	1.203111	172.16.0.8	64.13.134.52	TCP	58	36051	21	36051 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
24	1.203176	172.16.0.8	64.13.134.52	TCP	58	36051	5900	36051 → 5900 [SYN] Seq=0 Win=3072 Len=0 MSS=1460
25	1.203241	172.16.0.8	64.13.134.52	TCP	58	36051	587	36051 → 587 [SYN] Seq=0 Win=4096 Len=0 MSS=1460
26	1.203316	172.16.0.8	64.13.134.52	TCP	58	36051	995	36051 → 995 [SYN] Seq=0 Win=2048 Len=0 MSS=1460
27	1.203381	172.16.0.8	64.13.134.52	TCP	58	36051	1025	36051 → 1025 [SYN] Seq=0 Win=3072 Len=0 MSS=1460
28	1.203446	172.16.0.8	64.13.134.52	TCP	58	36051	111	36051 → 111 [SYN] Seq=0 Win=4096 Len=0 MSS=1460
29	1.203514	172.16.0.8	64.13.134.52	TCP	58	36051	199	36051 → 199 [SYN] Seq=0 Win=3072 Len=0 MSS=1460
30	1.203581	172.16.0.8	64.13.134.52	TCP	58	36051	3306	36051 → 3306 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31	1.203651	172.16.0.8	64.13.134.52	TCP	58	36051	143	36051 → 143 [SYN] Seq=0 Win=4096 Len=0 MSS=1460
32	1.203716	172.16.0.8	64.13.134.52	TCP	58	36051	443	36051 → 443 [SYN] Seq=0 Win=2048 Len=0 MSS=1460
33	1.402807	172.16.0.8	64.13.134.52	TCP	58	36050	1723	36050 → 1723 [SYN] Seq=0 Win=4096 Len=0 MSS=1460
34	1.402891	172.16.0.8	64.13.134.52	TCP	58	36050	993	36050 → 993 [SYN] Seq=0 Win=4096 Len=0 MSS=1460
35	1.402958	172.16.0.8	64.13.134.52	TCP	58	36050	110	36050 → 110 [SYN] Seq=0 Win=4096 Len=0 MSS=1460
36	1.403023	172.16.0.8	64.13.134.52	TCP	58	36050	8080	36050 → 8080 [SYN] Seq=0 Win=4096 Len=0 MSS=1460
37	1.403088	172.16.0.8	64.13.134.52	TCP	58	36050	1720	36050 → 1720 [SYN] Seq=0 Win=4096 Len=0 MSS=1460

(wireshark)

Some Abbreviations

srcip	Source IP
dstip	Destination IP
srcport	Source port of transport protocol
dstport	Destination port of transport protocol
proto	Transport protocol (according to *proto* field in Network protocol header)

How Do "Attacks" Look Like?

Flow point of view

TIMEFIRST	TIMELAST	SRCIP:SRCPORT	->	DSTIP:DSTPORT	PROTO	FLG	PKTS	#B
8:09	8:09	46.28.11.24:123	->	10.0.1.15:42958	UDP	.....	1	76
8:09	8:09	10.0.1.15:42958	->	46.28.11.24:123	UDP	.....	1	76
8:09	8:09	0.0.0.0:0	->	224.0.0.1:0	2	.....	1	32
8:09	8:09	10.0.1.1:53	->	10.0.1.15:46187	UDP	.....	2	344
8:10	8:10	10.0.1.1:0	->	10.0.1.15:0	ICMP	.....	199	208854
8:10	8:10	10.0.1.15:46501	->	10.0.1.1:53	UDP	.....	2	126
8:10	8:10	10.0.1.15:0	->	10.0.1.1:2048	ICMP	.....	199	208854
8:10	8:10	10.0.1.15:50645	->	10.0.1.1:53	UDP	.....	2	124
8:10	8:10	10.0.1.1:53	->	10.0.1.15:55978	UDP	.....	2	344
8:10	8:11	10.0.1.1:0	->	10.0.1.15:0	ICMP	.....	3096	3256202
8:10	8:11	10.0.1.15:0	->	10.0.1.1:2048	ICMP	.....	3096	3256202
8:10	8:11	10.0.1.1:22	->	10.0.1.15:34974	TCP	.AP...	2484	835296
8:10	8:11	10.0.1.15:34974	->	10.0.1.1:22	TCP	.AP...	1903	99652
8:11	8:11	10.0.1.1:53	->	10.0.1.15:56957	UDP	.....	2	242
8:09	8:12	10.0.1.220:5353	->	224.0.0.251:5353	UDP	.....	43	6665

How Do Attacks Look Like?

Alert point of view


```
{"Category": ["Malware"], "Node": [{"AggrWin": "00:05:00", "SW": ["
    Nemea", "urlblacklistfilter"], "Type": ["Flow", "Blacklist"], "
    Name": "cz.cesnet.nemea.urlblacklist"}], "EventTime":
    "2018-09-28T17:28:24Z", "Description": "URL: 'vseccz.weebly.com
    ' (listed: Malware Domains) was requested by 146.102.131.199.",
     "Format": "IDEA0", "CeaseTime": "2018-09-28T17:28:41Z", "
    CreateTime": "2018-09-28T17:30:58Z", "Note": "URL: 'vseccz.
    weebly.com' was found on blacklist(s): Malware Domains.", "
    Source": [{"InFlowCount": 4, "Proto": ["tcp"], "Hostname": "
    vseccz.weebly.com", "InByteCount": 3136, "InPacketsCount": 30,
    "IP4": ["199.34.228.53"], "Type": ["OriginBlacklist"], "Port":
    [443]}, {"IP4": ["146.102.131.199"], "Proto": ["tcp"]}], "
    DetectTime": "2018-09-28T17:28:41Z", "Ref": ["http://mirror1.
    malwaredomains.com/files/justdomains"], "ID": "aaf1206b-f7e7
    -419a-898b-72447a1ed72c"}
```

How Do Attacks Look Like?

Alert point of view

RealTime Events | Escalated Events

ST	CNT	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	2	2017-02-11 03:02:41	10.3.14.134	51734	10.3.14.2	53	17	ET DNS Query to a *.top domain - Likely Hostile
RT	4	2017-02-11 03:02:43	10.3.14.134	49249	104.155.4.180	80	6	ET INFO HTTP Request to a *.top domain
RT	1	2017-02-11 03:02:43	104.155.4.180	80	10.3.14.134	49249	6	ET POLICY PE EXE or DLL Windows file download
RT	1	2017-02-11 03:02:43	104.155.4.180	80	10.3.14.134	49249	6	ET POLICY Binary Download Smaller than 1 MB Likely Hostile
RT	2	2017-02-11 03:02:43	104.155.4.180	80	10.3.14.134	49249	6	ET CURRENT_EVENTS Likely Evil EXE download from MSXMLHTTP non-exe extension M2
RT	2	2017-02-11 03:02:43	104.155.4.180	80	10.3.14.134	49249	6	ET TROJAN JS/WSF Downloader Dec 08 2016 M6
RT	2	2017-02-11 03:02:43	104.155.4.180	80	10.3.14.134	49249	6	ET INFO Possible EXE Download From Suspicious TLD
RT	2	2017-02-11 03:02:43	104.155.4.180	80	10.3.14.134	49249	6	ET INFO EXE - Served Attached HTTP
RT	1	2017-02-11 03:02:44	10.3.14.134	51735	91.119.56.0	6892	17	ET TROJAN Ransomware/Cerber Checkin M3 (4)
RT	1	2017-02-11 03:02:44	10.3.14.134	51735	91.121.56.30	6892	17	ET TROJAN Possible Downadup/Conficker-C P2P encrypted traffic UDP Ping Packet (bit ...
RT	1	2017-02-11 03:02:50	10.3.14.134	51736	91.119.56.0	6892	17	ET TROJAN W32/Cerber.Ransomware CnC Checkin M4
RT	1	2017-02-11 03:02:54	10.3.14.134	49250	54.87.5.88	80	6	ETPRO TROJAN Cerber Blockchain Query
RT	2	2017-02-11 03:02:54	10.3.14.134	50205	10.3.14.2	53	17	ET TROJAN Ransomware/Cerber Onion Domain Lookup
RT	7	2017-02-11 03:03:21	67.210.245.241	80	10.3.14.131	49506	6	ET SHELLCODE UTF-8/16 Encoded Shellcode
RT	2	2017-02-11 03:03:21	67.210.245.241	80	10.3.14.131	49506	6	ET WEB_CLIENT Possible String.FromCharCode Javascript Obfuscation Attempt
RT	1	2017-02-11 03:04:07	10.3.14.131	49585	54.229.205.204	12080	6	ET POLICY HTTP Request on Unusual Port Possibly Hostile
RT	1	2017-02-11 03:04:07	10.3.14.131	49585	54.229.205.204	12080	6	ET POLICY HTTP POST on unusual Port Possibly Hostile
RT	2	2017-02-11 03:05:47	10.3.14.131	64890	10.3.14.2	53	17	ET TROJAN Spora Ransomware DNS Query

How Do Attacks Look Like?

Incident point of view in IODEFv2 — ex. C2 domains from a given campaign

https://tools.ietf.org/html/rfc7970#section-7.2

```
...
<IndicatorData>
  <Indicator>
    <IndicatorID name="csirt.example.com" version="1">G90823490</
        IndicatorID>
    <Description>C2 domains</Description>
    <StartTime>2014-12-02T11:18:00-05:00</StartTime>
    <Observable>
      <BulkObservable type="fqdn">
      <BulkObservableList>
        kj290023j09r34.example.com
        09ijk23jfj0k8.example.net
        klknjwfjiowjefr923.example.org
        oimireik79msd.example.org
      </BulkObservableList>
    </BulkObservable>
  </Observable>
</Indicator>
</IndicatorData>
...
```

Section 5

Closing Words

(Recommended) Resources

- Simon Hansman, Ray Hunt: *A taxonomy of network and computer attacks*, 2005, https://doi.org/10.1016/j.cose.2004.06.011.
- N. Hoque, Monowar H. Bhuyan, R.C. Baishya, D.K. Bhattacharyya, J.K. Kalita: *Network attacks: Taxonomy, tools and systems*, 2014, https://doi.org/10.1016/j.jnca.2013.08.001.

Questions?