

FOR578 – Cyber Threat Intelligence

Topics

Malware

Agent.BTZ	3-47
BlackEnergy	1-87
Kill chain	1-90-91
Version 2	1-88
Version 3	1-88-89
Carberp	1-10
Dark Seoul	3-80
DeputyDog	3-8
Derusbi	3-8
Evoltin	3-83
FYSBIS	5-15
Gh0stRat	3-8
GlassRAT	3-57
C2 overlap	3-58
Lessons Learned	3-59
Hikit	3-6-7, 3-8
Hydraq	3-8, 1-40
KillDisk	1-86
McRAT	3-6-7
Neodymium	1-66
Characteristics	1-68
Infection	1-69
NetWire	2-91
njRat	3-23
PlugX	3-5, 3-8, 3-23
PoisonIvy	3-5, 3-8, 2-14, 1-40
Promethium	1-66
Characteristics	1-68
Sogu	3-23
Truvasys	1-68
WebC2	2-25
Wingbird	1-68

Operation

Aurora	1-38
Blockbuster	4-84
Bodyguard	1-20
Flame	4-84
NightDragon Project	1-39
Shady RAT Project	1-39
SMN	3-10
Troy	4-80, 4-84

Commands

UnRAR	2-103
awk	2-93, 2-100
date	2-69
grep	2-69
net	2-33
openssl	2-25, 2-100
perl	2-100
ra	2-66, 2-84, 2-87
sed	2-100

Kill Chain	2-7, 1-31
KC1. Reconnaissance	2-9

KC2. Weaponization	2-13
KC3. Delivery	2-15
KC4. Exploitation	2-18
KC5. Installation	2-20
KC6. Command-and-Control	2-23
KC7. Actions on Objectives	2-26, 2-81

Vulnerability

CVE-2014-0160	2-18
CVE-2014-1761	3-110
CVE-2014-6271	2-18
CVE-2014-7169	2-18
CVE-2016-4117	1-68

#

0-Day exploit	1-40
---------------------	------

A

Abstractions	1-44
Actions on Objectives	2-26, 2-81
Example	2-28
Active Defense	1-73
Active Measures	5-95
Activity Group	1-45, 1-50, 4-75
Activity group	1-70
Advanced Persistent Threat	2-31
Adversary	1-45, 1-47
Adversary Admission	5-79
AlienVault OTX	3-63
Analysis	1-24
Type	1-27
Analysis of Competing Hypothesis	4-33-34
Hypotheses	4-35
Evidences	4-36
Diagnostics	4-37
Refinement	4-38
Inconsistency	4-39
Sensitivity	4-40
Report	4-41
Analyst	1-7
Analyst's Notebook	4-47
Analytical Model	5-81, 5-89
Anti-Virus	2-21
Apache Solr	4-55
Apache Tika	4-55
Architecture	1-73
Argus	2-65, 2-87
ASN	3-40
Assessment	5-66
Attribution	5-77-78
ACH	5-92
Approaches	5-79
Intent	5-87
Issues	4-86
Matrix	5-92
State	5-88
State Responsibility	5-83

FOR578 – Cyber Threat Intelligence

Use cases	5–82
Value without Attribution	5–81
Audience	5–5, 1–97–98
Automater	3–68
AWS	2–10
Axiom (Team)	3–8
Axioms	1–44, 5–97

B

Backdoor	2–13
Base64	2–25
Beaconing	2–24
Bias	4–17, 1–28
Anchoring	4–22
Cognitive Biases	4–21
Confirmation Bias	4–23
Congruence Bias	4–24
Example	1–29
Field of view	1–34
Hindsight Bias	4–25
Illusory Correlation	4–26
Bit9	3–6–7
BPF	2–84
Brainstorming	1–30

C

Cambridge Intelligence	4–47
Campaign	1–45, 1–52
Heatmap	5–44
Capability	3–12, 2–33, 1–47
Carbanak	1–9, 1–11
C2	1–13
Evolution	1–13
Impact	1–14
Lazarus	4–84
Lessons Learned	1–15
Overview	1–12
Censys.io	3–106
Centrifuge	4–47
ChangeIP	3–35–36
ChopShop	2–90
CIDR	2–52
CIF → Collective Intelligence Framework	
CIRCL	3–106
Clark, Robert	1–113
Cloud	2–10
Clustering	4–68
CMF → Collection Management Framework	
Collection	1–107
Management Framework	1–108–109
Collective Intelligence Framework	3–65
Combine	3–64
Command-and-Control	2–23, 2–90
Example	2–25
Completeness	5–48

Confidence Assessment	5–65
Correlation and Causation	4–28
Counter-Intelligence	1–19
Defensive	1–20
Example	1–20
Offensive	1–20
Course of Action	2–38
Active	2–47
Deceive	2–45
Degrade	2–44
Deny	2–42
Destroy	2–46
Detect	2–41
Discover	2–40
Disrupt	2–43
Matrix	2–39
Passive	2–47
Selection and Exclusivity	2–47
CRITS	4–9
Cum hoc ergo propter hoc	4–28
Customer	2–32
CVE	2–18
Cyber Threat Intelligence	1–43, 1–73
Elements	1–44
Levels	1–97–98
Storage	4–9
(Best practice)	4–14
Terminology	1–45
CyberChef	3–71
CyBOX	5–31

D

Data Analysis	4–49
Data to Intelligence	1–35
DataSploit	3–69
DBIR	1–119
DC3 → Defense Cyber Crime Centre	
Deception	5–95
Defense Cyber Crime Centre (DC3)	3–22
Delivery	2–15
Example	2–16
Detection	2–139
Devil Advocate	1–30
Diamond Model	2–29, 1–50
Activity Group	4–76
Adversary	2–32
Analytic Findings	5–64
Axiom	2–30–31
Capability	2–33
Clustering	4–71
Infrastructure	2–34
Meta-Features	4–74
Tactics, Techniques, and Procedures (TTP)	2–33
Victim	2–35
Direct Access	5–79
Discover	3–69
Disinformation	5–96

FOR578 – Cyber Threat Intelligence

Disk Image	2-106
Domains	3-33
Compromise	3-38
DomainTools	3-43, 3-52-53
Dropper	2-13, 2-20
Dshell	2-90
DShield	3-62
Dual Maps	3-72
Dynamic DNS	3-35
DynDns	3-35

E

Elderwood Project	1-39
Email Delivery Success Metric	5-47
Estimative Language	5-60
Estimative Scale	5-62
Evidenciary Dependency	4-40
Exfiltration	2-103
Exploit	2-18
Exploitation	2-18
Example	2-19

F

Fallacies	4-17
Anecdotal Fallacies	4-18
Appeal to Probability	4-18
Appeal to the Stone	4-19
Argument from Repetition	4-19
Argument from Silence	4-19
Burden of Proof	4-20
Common Fallacies	4-20
Informal Fallacies	4-19
Logical Fallacies	4-18
Moddle Ground	4-20
Farsight	3-43
FinFisher	1-70
Flow ratio	2-87
Forensics	
Disk	2-94
Memory	2-93
FTP	2-86
Full Packet Capture	2-85

G

GEOINT	1-18, 3-72
Gephi	4-47
Google	1-13
Google Maps	3-72
Graphviz	4-47
Guardian of Peace	4-81
GULP	2-85

H

HackingTeam	4-5-7
Whois	4-80
HeartBleed	2-18
Heuer, Richards J. Jr	1-23
High-Impact/Low Probability Analysis	1-30
HTTP Headers	2-16
HUMINT	1-18
Hypothesis Generation	4-58, 1-75

I

idc.py	5-10
Identifier	4-62
Incident (One-slider)	5-45
Incident Response	2-57, 2-140
Indicator	1-45, 1-58
Discovery	1-64
Fatigue	1-65
Key indicators	1-62-63
Life Cycle	2-40, 1-59
Lifespan	1-64
To Behavioral Analytics	1-81
Validation	5-21
Indicator Life Cycle	2-75
Indicators	2-135
InfoGo	3-69
Information	1-35
InfraGuard	5-27
Infrastructure	
Acquisition	2-9
Installation	2-20
Example	2-21
Intelligence	1-17, 1-35
Axioms	5-97
Funnel	1-35
Gain/Loss	2-47
Sources	1-18
Intelligence Consumption	1-72
Active Defense	1-76
Architeture	1-78
Intelligence	1-75
Passive Defense	1-77
To Generation	1-95
Intelligence Generation	1-72
From Consumption	1-95
Intelligence Life Cycle	5-86
Intelligence Team	
Example	1-100
Interactions	1-99
Process	1-101
Intent	2-34, 1-47
Attribution	5-87
Internet Identity	3-43
Interpretation	5-58
Intrusion	1-45, 1-49
Analysis	5-79
Clustering	4-68
IP Address	2-52

FOR578 – Cyber Threat Intelligence

ISACs 5-28
ISAOs 5-29

J

Judgment 1-25

K

Kent, Sherman 1-21
 Doctrine 1-22
KeyLines 4-47
Kill Chain
 Clustering 4-71
 Completion 2-78
 Multiple 1-118
 Sequencing 1-128

L

LaBrea 2-44
Layer 5 Protocols 2-70
Lazarus 4-84
Leaks 5-79
Lessons Learned 1-41
libyara 5-10
Lifecycle 1-32
Link Analysis 4-46
 Tools 4-47
Linkurious 4-47, 4-55
logrotate 2-55
Logs 2-55, 2-107
 Proxy 2-68
Looking Glass LGScout 3-43

M

MAC → Modification, Access, Change Time 2-21
MAEC 5-32
Maltego 3-27, 4-47, 3-73
 Transforms 3-74-80
Malware 3-12
 Commodity 1-15
 Configuration 3-21
 Zoos 3-13
Malware Analysis 2-96
MalwR 3-13
MASINT 1-18
Memory Analysis 2-57
Memory Image 2-106
Mental Models 1-30
MetaSploit 2-13
Metrics 5-42
MISP 4-11-13
Mitigation Scorecard 5-46
MITRE ATT&CK 2-142

Tactic 2-142
Technique 2-143
MITRE Threat Groups 4-64
Mnemonic 3-43, 3-45

N

Name 4-62
Neo4J 4-47, 4-55
NetFlows 2-65
New Romantic Cyber Army 4-80
New-York Stock Exchange Glitch 4-27
Nuix 4-55

O

Observation 5-58
Offense 1-73-74
OpenDNS 3-43
Operational Threat Intelligence 5-25, 1-97-98
Operator 2-32
Opportunity 1-47, 5-91
Oray 3-35
Organizational Research 2-9
OSINT 1-18, 3-67
 Geographical information 3-72
 Tools 3-67-68

P

Packing 2-18
Palantir 4-47
Panama Papers 4-53
Passive Defense 1-73
Passive DNS 3-42, 3-44
PassiveTotal 3-43, 3-106
Perception 1-26
Persona 1-45, 1-54, 2-102
Pivot 3-28
 Accounts 3-29
 Command and control 2-90
 Disk 2-94
 Domains 3-29, 3-33
 Host 2-83
 IP address 3-29
 Memory 2-92
 Network 2-82
 Unique Strings 3-29
PLA Unit 61398 1-39
Playbook 2-140
Poison Hurricane 3-39
Power Grid 1-84
 Ukraine Power Outage 1-85
Prefetch 2-95, 2-122
Prevention 2-138
Primitives 1-44
Proxy 2-68
Pyramid of pain 1-82

FOR578 – Cyber Threat Intelligence

R

RapidPivot	3-27
RAT	2-23
Reconnaissance	2-9
Example	2-11
Recorded Future	3-95-98
Red Team	1-30, 1-75
RedLine	2-57
Report	5-57
Pros and Cons	5-70, 5-72, 5-75
Requirements	1-45, 1-48, 1-95
Prioritization	1-96
Reassess	5-94
Requirements, Intelligence	1-110
Reverse Engineering	2-96
RFC1918	2-52
RFI	1-32
RiskIQ	3-43
RookSecurity	4-7
RSA SecurID	1-39
Russia - Georgia	5-84

S

SANS Internet Storm Center	3-62
Saudi Aramco	5-84
SCADA	1-84
Scale of Cyber Security	1-73
Scans.io	3-106
Shadow Brokers	4-57
Sharing	
Best practice	5-39
National-level Government Information	5-27
Partners and Collaboration	5-26
ShellShock	2-18
Shodan	3-70
SIEM	2-55
Siemens	1-88
SIGINT	1-18
Simatic	1-88
Simpsons	5-80
Situational Awareness	5-49
Snake	3-47
Sofacy	5-15
Bundestag	5-18
Sony	5-84
Sony Attack	4-81-83
Spearphishing	1-40
Spectrum of State Responsibility	5-83
Squid	2-68
STIX	5-31
1.0	5-35
2.0	5-36
Repository	5-37
Strategic	1-97-98
Strategic Threat Intelligence	5-53
Expectations	5-55

Structured Analytic Technique	1-30
syslog	2-55

T

Tactical Threat Intelligence	1-97-98
Tactics, Techniques, and Procedures (TTP)	1-45, 1-55
Target	1-45
Target Identification	2-9
Target-Centric Analysis	1-113
Tarpitting	2-44
Tasking	2-9
TAXII	5-31
Implementation	5-34
Repository	5-37
Team A/B	1-30
Temporal clustering	2-107
Temporal Data Analysis	4-50-51
Temporal triangulation	2-107
Thinking	1-26
Threat	1-45, 1-47
Definition	5-90
Threat Actor	1-45, 1-51
Threat Behavior	2-135
General vs. Activity group	2-141
Threat Data Feeds	3-61
Pros and Cons	3-66
Threat Detection	
Approaches	2-135
Types	1-80
Threat Groups	
Mapping	4-66-67
Rosetta Stone	4-65
Threat Intelligence Platforms	4-10
Threat Modeling	1-111-112, 1-117, 2-137
Example	1-114-116
Granularity	1-118
Steps	1-114
Threat_Note	4-9
ThreatCrowd	3-77, 3-80
TIF → Temporary Internet Files	2-123
Titan	4-47
TLP → Traffic Light Protocol	
TLS Certificate	3-103
Compromise	3-57
Datastores	3-104
Pivot	3-107
Tools (Acquisition, Recon)	2-9
Tools and Tradecraft	1-40
Tradecraft	1-45, 1-56
Traffic Light Protocol (TLP)	1-45, 1-53
Trend Analysis	4-52
Trojan	2-23
TTP → Tactics, Techniques, and Procedures	
Turkey Pipeline Explosion	4-29
Turla	3-47
Types of analysis	4-45

FOR578 – Cyber Threat Intelligence

U

URL	2-72
Uroburos	3-47
US-CERT	5-27

V

VERIS	1-119-121
Verizon Data Breach	1-119
Victim	1-45
VirusTotal	3-14-20
Volatility	2-57, 2-92-93

W

WannaCry	4-85
Watering hole	1-40
Weaponization	2-13

Example	2-14
---------------	------

WFP → Windows File Protection	2-21
-------------------------------------	------

Whois	3-34
-------------	------

Whois HackingTeam	4-80
-------------------------	------

Wireshark	2-86
-----------------	------

Y

YARA	5-6
------------	-----

Alternative	5-9
-------------------	-----

Extensions	5-10
------------------	------

filesize	5-12
----------------	------

Import	5-11
--------------	------

Jump	5-9
------------	-----

Key points	5-8
------------------	-----

MZ	5-12
----------	------

Reference	5-11
-----------------	------

Rule (example)	5-7
----------------------	-----

yarascan	5-10
----------------	------

yextend	5-10
---------------	------