MISP taxonomies and classification as machine tags

Table of Contents

Introduction

The MISP threat sharing platform is a free and open source software helping information sharing of threat intelligence including cyber security indicators, financial fraud or counter-terrorism information. The MISP project includes multiple sub-projects to support the operational requirements of analysts and improve the overall quality of information shared.

Taxonomies that can be used in MISP (2.4) and other information sharing tool and expressed in Machine Tags (Triple Tags). A machine tag is composed of a namespace (MUST), a predicate (MUST) and an (OPTIONAL) value. Machine tags are often called triple tag due to their format. The following document is generated from the machine-readable JSON describing the MISP taxonomies.

Funding and Support

The MISP project is financially and resource supported by CIRCL Computer Incident Response Center Luxembourg .

A CEF (Connecting Europe Facility) funding under CEF-TC-2016-3 - Cyber Security has been granted from 1st September 2017 until 31th August 2019 as **Improving MISP as building blocks for next-generation information sharing**.

If you are interested to co-fund projects around MISP, feel free to get in touch with us.

MISP taxonomies

CERT-XLM

CERT-XLM namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

CERT-XLM Security Incident Classification.

abusive-content

Abusive Content.

CERT-XLM:abusive-content="spam"

spam

Spam or 'unsolicited bulk e-mail', meaning that the recipient has not granted verifiable permission for the message to be sent and that the message is sent as part of a larger collection of messages, all having identical content.

CERT-XLM:abusive-content="harmful-speech"

Harmful Speech

Discretization or discrimination of somebody (e.g. cyber stalking, racism and threats against one or more individuals) May be found on a forum, email, tweet etc...

CERT-XLM:abusive-content="violence"

Child/Sexual/Violence/...

Any Child pornography, glorification of violence, may be found on a website, forum, email, tweet etc...

malicious-code

Software that is intentionally included or inserted in a system for a harmful purpose. A user interaction is normally necessary to activate the code.

CERT-XLM:malicious-code="virus"

Virus

Malicious code that replicate itself and infects the computer and files;

CERT-XLM:malicious-code="worm"

Worm

Malware that self-replicates and spread itself to other computers in the network without any user interaction;

CERT-XLM:malicious-code="ransomware"

Ransomware

Ransomware is a type of malicious software from cryptovirology that blocks access to the victim's data or threatens to publish it until a ransom is paid.

CERT-XLM:malicious-code="trojan-malware"

Trojan/Malware

This category regroups many common malware types (Banking, POS, Mining malware).

CERT-XLM:malicious-code="spyware-rat"

Spyware/Rat

This category regroups malware types and tools that may have a bigger impact on the breached infrastructure and usually need further investigations (Common Spyware/Rat, State sponsored malwares, StealersHacking tool).

CERT-XLM:malicious-code="dialer"

Dialer

Computer program used to identify the phone numbers that can successfully make a connection with a computer modem. Use this category to classify overpriced SMS sent by malicious mobile application.

CERT-XLM:malicious-code="rootkit"

Rootkit

Malware, which alter the standard functionality of an operating system in order to do its malicious actions in a stealthy way. In practice, Rootkits hijacks systems functions in order to alter the returning values to hide themselves from simple analysis tools.

information-gathering

This group is for the reconnaissance; generally, it is the step before attacking.

CERT-XLM:information-gathering="scanner"

Scanning

Attacks that send requests to a system to discover weak points. This also includes some kinds of testing processes to gather information about hosts, services and accounts. Examples: fingerd, DNS querying, ICMP, SMTP (EXPN, RCPT,).

CERT-XLM:information-gathering="sniffing"

Sniffing

Observing and recording network traffic (wiretapping).

CERT-XLM:information-gathering="social-engineering"

Social Engineering

Gathering information from a human being in a non-technical way (eg, lies, tricks, bribes, or threats).

intrusion-attempts

This group is for attack detected/tried but without success.

CERT-XLM:intrusion-attempts="exploit-known-vuln"

Exploiting known vulnerabilities

An attempt to compromise a system or to disrupt any service by exploiting vulnerabilities with a standardised identifier such as CVE name (eg, buffer overflow, backdoors, cross side scripting, etc).

CERT-XLM:intrusion-attempts="login-attempts"

Login attempts

Multiple login attempts (guessing / cracking of passwords, brute force).

CERT-XLM:intrusion-attempts="new-attack-signature"

New attack signature

An attempt using an unknown exploit.

intrusion

This group is for successful unauthorized access to a system.

CERT-XLM:intrusion="privileged-account-compromise"

Privileged Account Compromise

A successful full compromise of a system or application (service). This can have been caused remotely by a known or new vulnerability, but also by an unauthorized local access.

CERT-XLM:intrusion="unprivileged-account-compromise"

Unprivileged Account Compromise

A successful compromise of a system or application (service). This can have been caused remotely by a known or new vulnerability, but also by an unauthorized local access. The intruded did not achieve to escale his privileges locally.

CERT-XLM:intrusion="botnet-member"

Botnet member

The compromised asset is also being part of a botnet. This is reserved mainly for public web servers. See malicious code in priority for workstations or internal server's compromise. For example, phpmailer, etc…

CERT-XLM:intrusion="domain-compromise"

Domain Compromise

The whole domain is compromised; this is commonly used for active directory and detected by a "pass the ticket" attack or a discovery of "ad dumps" files.

CERT-XLM:intrusion="application-compromise"

Application Compromise

An application is compromised; the attacker possess an uncontrolled access to data, server, and assets used by this application (CMDB, DB, Backend services, etc.).

availability

By this kind of an attack a system is bombarded with so many packets that the operations are delayed or the system crashes.

CERT-XLM:availability="dos"

DoS

An attacker attempts to prevent legitimate users from accessing information or services.

CERT-XLM:availability="ddos"

DDoS

Form of electronic attack involving multiple computers, which send repeated requests (HTTP requests, pings, TCP or UDP Flood) to a server to load it down and render the service inaccessible for a period of time.

CERT-XLM:availability="sabotage"

Sabotage

Deliberate and malicious acts that result in the disruption of the normal processes and functions or the destruction or damage of equipment or information.

CERT-XLM:availability="outage"

Outage (no malice)

Unavailability of the system but done with no malice.

information-content-security

This group is dealing with non-legitimate access or modification to data.

CERT-XLM:information-content-security="Unauthorised-information-access"

Unauthorised access to information

Any access to unauthorized data. It may be access of data on improperly restricted server share or database exfiltered by using a SQLi.

CERT-XLM:information-content-security="Unauthorised-information-modification"

Unauthorised modification of information

Unauthorized tampering of data on files, documents or database.

fraud

This group is for unauthorized use of resources using resources for unauthorized purposes including profit-making ventures (eg, the use of e-mail to participate in illegal profit chain letters or pyramid schemes).

CERT-XLM:fraud="copyright"

Copyright

Selling or installing copies of unlicensed commercial software or other copyright protected materials (Warez).

CERT-XLM:fraud="masquerade"

Masquerade

Types of attacks in which one entity illegitimately assumes the identity of another in order to benefit from it. This attack may be used for president fraud requesting transactions.

CERT-XLM:fraud="phishing"

Phishing

Masquerading as another entity in order to persuade the user to reveal a private credential.

vulnerable

Vulnerable

CERT-XLM:vulnerable="vulnerable-service"

Open for abuse

Open resolvers, world readable printers, vulnerability apparent from Nessus etc scans, virus, signatures not up to date, etc. This includes for example default SNMP community or default password on any application.

conformity

This group is for catching breach about controls given by the company or externals entities.

CERT-XLM:conformity="regulator"

Regulator

All lack about regulator rules (CSSF, GDPR, etc.).

CERT-XLM:conformity="standard"

Standard

All lack about standards certification of the company (ISO27000, NIS, ISAE3402, etc.).

CERT-XLM:conformity="security-policy"

Security policy

All lack about the internal security policy of the company.

CERT-XLM:conformity="other-conformity"

Other

All lack that do not fit in one of previous categories should be put on this class.

other

Other

CERT-XLM:other="other"

other

All incidents that do not fit in one of the given categories should be put into this class. If the number of incidents in this category increases, it is an indicator that the classification scheme must be revised.

test

Meant for testing.

DML

DML namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

The Detection Maturity Level (DML) model is a capability maturity model for referencing ones maturity in detecting cyber attacks. It's designed for organizations who perform intel-driven detection and response and who put an emphasis on having a mature detection program.

8

If the actor is part of a larger organized operation they may be receiving their goals from a higher level source or handler. Depending on how organized and sophisticated the adversary's campaigns are, these goals may not even be shared with the operator(s) themselves. In cases of non-targeted threat actors, this may be much less organized or distributed. Goals are nearly impossible to detect (directly) but they're almost always the toughest question C-level leaders ask about post-breach. "Who was it and why?" These kinds of questions can never truthfully be answered unless you're operating at Detection Maturity Level 8 against your adversary and can prove reliably that you know what their goals are. Short of that, it's guessing at what the adversary's true intentions were based on behavioral observations made at lower DMLs (e.g. data stolen, directories listed, employees or programs targeted, etc). I anticipate less than a handful of organizations truly operate at this level, consistently, against the threat actors they face because it's nearly impossible to detect based on goals alone.

DML:8

Goals

If the actor is part of a larger organized operation they may be receiving their goals from a higher level source or handler. Depending on how organized and sophisticated the adversary's campaigns are, these goals may not even be shared with the operator(s) themselves. In cases of non-targeted threat actors, this may be much less organized or distributed. Goals are nearly impossible to detect (directly) but they're almost always the toughest question C-level leaders ask about post-breach. "Who was it and why?" These kinds of questions can never truthfully be answered unless you're operating at Detection Maturity Level 8 against your adversary and can prove reliably that you know what their goals are. Short of that, it's guessing at what the adversary's true intentions were based on behavioral observations made at lower DMLs (e.g. data stolen, directories listed, employees or programs targeted, etc). I anticipate less than a handful of organizations truly operate at this level, consistently, against the threat actors they face because it's nearly impossible to detect based on goals alone.

7

```
 If the adversary's high level goal is to "replicate Acme Company's Super Awesome
Product Foo in 2 years or less" their supporting strategies might include:
1.  Implant physical persons into the companies that produce this technology, in
positions with physical access to the information necessary to fulfill this goal.
2.  Compromise these organizations via cyber attack, and exfiltrate data from the
systems containing the information necessary to fulfill this goal.
For less targeted attacks, the strategy may be completely different, with shorter
durations or different objectives. The important distinguishing factor about Goals
(DML-8) and Strategy (DML-7) is that they are largely subjective in nature.  They are
very non-technical, and are often reflective of the adversary's (or their handler's)
true intentions (and strategies for fulfilling those intentions).  They represent what
the adversary wants.  For these reasons, they are not easily detectable via
conventional cyber means for most private organizations.   It's very common for DML-8
or DML-7 to not even be on the day-to-day radar of most Detection or Response
specialists, and if they are it's typically in the context of having received a
strategic intelligence report from an intelligence source about the adversary.
```

DML:7

Strategy

```
 If the adversary's high level goal is to "replicate Acme Company's Super Awesome
Product Foo in 2 years or less" their supporting strategies might include:
1.  Implant physical persons into the companies that produce this technology, in
positions with physical access to the information necessary to fulfill this goal.
2.  Compromise these organizations via cyber attack, and exfiltrate data from the
systems containing the information necessary to fulfill this goal.
For less targeted attacks, the strategy may be completely different, with shorter
durations or different objectives. The important distinguishing factor about Goals
(DML-8) and Strategy (DML-7) is that they are largely subjective in nature.  They are
very non-technical, and are often reflective of the adversary's (or their handler's)
true intentions (and strategies for fulfilling those intentions).  They represent what
the adversary wants.  For these reasons, they are not easily detectable via
conventional cyber means for most private organizations.   It's very common for DML-8
or DML-7 to not even be on the day-to-day radar of most Detection or Response
specialists, and if they are it's typically in the context of having received a
strategic intelligence report from an intelligence source about the adversary.
```

6

To successfully operate at DML-6, one must be able to reliably detect a tactic being employed regardless of the Technique or Procedure used by the adversary, the Tools they chose to use, or the Artifacts and Atomic Indicators left behind as a result of employing the tactic. While this may sound impossible on the surface, it absolutely is possible. In nearly all cases, tactics are not detected directly by a single indicator or artifact serving as the smoking gun, or a single detection signature or analytic technique. Tactics become known only after observation of multiple activities in aggregate, with respect to time and circumstance. As a result, detection of tactics are usually done by skilled analysts, rather than technical correlation or analytics systems.

DML:6

Tactics

To successfully operate at DML-6, one must be able to reliably detect a tactic being employed regardless of the Technique or Procedure used by the adversary, the Tools they chose to use, or the Artifacts and Atomic Indicators left behind as a result of employing the tactic. While this may sound impossible on the surface, it absolutely is possible. In nearly all cases, tactics are not detected directly by a single indicator or artifact serving as the smoking gun, or a single detection signature or analytic technique. Tactics become known only after observation of multiple activities in aggregate, with respect to time and circumstance. As a result, detection of tactics are usually done by skilled analysts, rather than technical correlation or analytics systems.

5

From a maturity perspective, being able to detect an adversary’s techniques is superior to being able to detect their procedures. The primary difference being techniques are specific to an individual. So when respecting this distinction, the ability to detect a specific actor operating within your environment by technique exclusively is an advantage. The best analogy to this is a rifled

barrel, which leaves uniquely identifiable characteristics in the side of a bullet. Because of this, ballistics specialists can forensically match a spent round to the exact weapon from which it was fired with a high degree of certainty. Not just any weapon by calibur or model, but the exact weapon used to fire that specific round. Human beings are creatures of habit, and most adversaries aren't aware of the fact that every time they attack they're leaving evidence of their personal techniques behind for us to find. The same applies for the tool builders writing the tools these adversaries use. It's our obligation to find these distinctions and ensure we're looking for them. It's personal behavior and habits that are the hardest for humans to change, so put the hurt on your adversaries by finding creative ways to detect their behaviors and habits in your environment.

DML:5

Techniques

From a maturity perspective, being able to detect an adversary's techniques is superior to being able to detect their procedures. The primary difference being techniques are specific to an individual. So when respecting this distinction, the ability to detect a specific actor operating within your environment by technique exclusively is an advantage. The best analogy to this is a rifled barrel, which leaves uniquely identifiable characteristics in the side of a bullet. Because of this, ballistics specialists can forensically match a spent round to the exact weapon from which it was fired with a high degree of certainty. Not just any weapon by calibur or model, but the exact weapon used to fire that specific round. Human beings are creatures of habit, and most adversaries aren't aware of the fact that every time they attack they're leaving evidence of their personal techniques behind for us to find. The same applies for the tool builders writing the tools these adversaries use. It's our obligation to find these distinctions and ensure we're looking for them. It's personal behavior and habits that are the hardest for humans to change, so put the hurt on your adversaries by finding creative ways to detect their behaviors and habits in your environment.

4

Given today's detection technology, and readily available correlation and analytics techniques, it's amazing that more organizations haven't reached Detection Maturity Level 4 for most of their adversaries. Procedures are one of the most effective ways of detecting adversary activity and can really inflict the most pain against lesser experienced "B-teams". In it's most simple form, detecting a procedure is as simple as detecting a sequence of two or more of the individual steps employed by the actor. The goal here is to isolate activities that the adversary appears to perform methodically, two or more times during an incident.

DML:4

Procedures

Given today's detection technology, and readily available correlation and analytics techniques, it's amazing that more organizations haven't reached Detection Maturity Level 4 for most of their adversaries. Procedures are one of the most effective ways of detecting adversary activity and can really inflict the most pain against lesser experienced "B-teams". In it's most simple form, detecting a procedure is as simple as detecting a sequence of two or more of the individual steps employed by the actor. The goal here is to isolate activities that the adversary appears to perform methodically,

two or more times during an incident.

3

Being able to detect at DML-3 means you can reliably detect the adversary's tools, regardless of minor functionality changes to the tool, or the Artifacts or Atomic Indicators it may leave behind. Detecting tools falls into two main areas. The first is detecting the transfer and presence of the tool. This includes being able to observe the tool being transferred over the network, being able to locate it sitting at rest on a file system, or being able to identify it loaded in memory. The second, and more important area of tool detection, is detecting the tool reliably by functionality. For example, let's take a given webshell that has 25 functions. If we want to claim DML-3 level detection for this webshell we have to exercise each of those 25 functions and understand what each of them do. What do they look like at the host, network, and event log level when they are exercised? We then aim to build detections for as many of those 25 functions across those data domains as we possibly can, reliably, balancing false positives and other constraints. The reason behind this is simple, we want to be able to detect this version of the tool and as many future variants of the tool as we can by function that it performs. If the adversary decides to change up 5 of the 25 functions for which we have detections, we're still detecting the entire tool. In order for the adversary to use this tool completely undetected in our environment, they'll be forced to change every one of those functions; or at least the ones that we were able to reliably build detections against.

DML:3

Tools

Being able to detect at DML-3 means you can reliably detect the adversary's tools, regardless of minor functionality changes to the tool, or the Artifacts or Atomic Indicators it may leave behind. Detecting tools falls into two main areas. The first is detecting the transfer and presence of the tool. This includes being able to observe the tool being transferred over the network, being able to locate it sitting at rest on a file system, or being able to identify it loaded in memory. The second, and more important area of tool detection, is detecting the tool reliably by functionality. For example, let's take a given webshell that has 25 functions. If we want to claim DML-3 level detection for this webshell we have to exercise each of those 25 functions and understand what each of them do. What do they look like at the host, network, and event log level when they are exercised? We then aim to build detections for as many of those 25 functions across those data domains as we possibly can, reliably, balancing false positives and other constraints. The reason behind this is simple, we want to be able to detect this version of the tool and as many future variants of the tool as we can by function that it performs. If the adversary decides to change up 5 of the 25 functions for which we have detections, we're still detecting the entire tool. In order for the adversary to use this tool completely undetected in our environment, they'll be forced to change every one of those functions; or at least the ones that we were able to reliably build detections against.

2

DML-2 is where most organizations spend too much of their resources; attempting to collect what they call "threat intelligence" in the form of Host & Network Artifacts. The reality is, these are merely just indicators that are observed either during or after the attack. They're like symptoms of

the flu but not the flu itself. I often use the analogy "chasing the vapor trail" when I think of DML-2 because chasing after Host & Network Artifacts is much like chasing the vapor trail behind an aircraft. We know the enemy aircraft is up there in front of us somewhere, if we just keep chasing this vapor trial we'll eventually catch up to the aircraft and find our enemy right? Wrong. Having a mature detection and response program means your operating above DML-2 and you're actually locked onto the aircraft itself. You know how it operates, you know what it's capabilities are, you know the Tactics, Techniques, and Procedures of it's pilot and you can almost predict what it's next moves might be. This is precisely why good Cyber Intelligence Analysts will almost never attribute activity to a specific threat actor, group, or country based on just Host & Network Artifacts alone; they understand this DML concept and realize when they're likely just staring at the vapor trail. They understand that in reality the vapor trail (indicators) could be from any number of aircraft (tools), with any number of pilots (actors) behind the stick.

DML:2

Host & Network Artifacts

DML-2 is where most organizations spend too much of their resources; attempting to collect what they call "threat intelligence" in the form of Host & Network Artifacts. The reality is, these are merely just indicators that are observed either during or after the attack. They're like symptoms of the flu but not the flu itself. I often use the analogy "chasing the vapor trail" when I think of DML-2 because chasing after Host & Network Artifacts is much like chasing the vapor trail behind an aircraft. We know the enemy aircraft is up there in front of us somewhere, if we just keep chasing this vapor trial we'll eventually catch up to the aircraft and find our enemy right? Wrong. Having a mature detection and response program means your operating above DML-2 and you're actually locked onto the aircraft itself. You know how it operates, you know what it's capabilities are, you know the Tactics, Techniques, and Procedures of it's pilot and you can almost predict what it's next moves might be. This is precisely why good Cyber Intelligence Analysts will almost never attribute activity to a specific threat actor, group, or country based on just Host & Network Artifacts alone; they understand this DML concept and realize when they're likely just staring at the vapor trail. They understand that in reality the vapor trail (indicators) could be from any number of aircraft (tools), with any number of pilots (actors) behind the stick.

1

These are the atomic particles that make up Host & Network artifacts. If you're detecting at Detection Maturity Level 1, it means you are probably taking "feeds of intel" from various sharing organizations and vendors in the form of lists, like domains and IP addresses, and feeding them into your detection technologies. Let me be clear on my position here. There are a few, and I mean a very precious few, circumstances where this makes sense and can be done reliably. These are edge cases where specific atomic indicators have a high enough "shelf life" where it makes sense to go ahead and create detection capabilities from them. Examples of this include unique strings found inside a binary, or perhaps an adversary is foolish enough to sit on the same recon, delivery, C2, or exfiltration infrastructure allowing you to detect reliably on their domain names or IP addresses. These might be viable cases where detecting on atomic indicator alone makes sense. Unfortunately, for the remaining 99% of the time, attempting to detect on this kind of data is suboptimal, for a number of reasons.

DML:1

Atomic IOCs

These are the atomic particles that make up Host & Network artifacts. If you're detecting at Detection Maturity Level 1, it means you are probably taking "feeds of intel" from various sharing organizations and vendors in the form of lists, like domains and IP addresses, and feeding them into your detection technologies. Let me be clear on my position here. There are a few, and I mean a very precious few, circumstances where this makes sense and can be done reliably. These are edge cases where specific atomic indicators have a high enough "shelf life" where it makes sense to go ahead and create detection capabilities from them. Examples of this include unique strings found inside a binary, or perhaps an adversary is foolish enough to sit on the same recon, delivery, C2, or exfiltration infrastructure allowing you to detect reliably on their domain names or IP addresses. These might be viable cases where detecting on atomic indicator alone makes sense. Unfortunately, for the remaining 99% of the time, attempting to detect on this kind of data is suboptimal, for a number of reasons.

0

For organizations who either don't operate at DML-1 or higher, or they don't even know where they operate on this scale, we have Detection Maturity Level - 0. Instead of pointing out all the negative things associated with this level, I'll take the high road and lend a bit of positive encouragement. Congratulations, you are at ground zero. It can only get better from here.

DML:0

None or Unknown

For organizations who either don't operate at DML-1 or higher, or they don't even know where they operate on this scale, we have Detection Maturity Level - 0. Instead of pointing out all the negative things associated with this level, I'll take the high road and lend a bit of positive encouragement. Congratulations, you are at ground zero. It can only get better from here.

PAP

PAP namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

The Permissible Actions Protocol - or short: PAP - was designed to indicate how the received information can be used.

RED

PAP:RED

(PAP:RED) Non-detectable actions only. Recipients may not use PAP:RED information on the network. Only passive actions on logs, that are not detectable from the outside.

AMBER

PAP:AMBER

(PAP:AMBER) Passive cross check. Recipients may use PAP:AMBER information for conducting online checks, like using services provided by third parties (e.g. VirusTotal), or set up a monitoring honeypot.

GREEN

PAP:GREEN

(PAP:GREEN) Active actions allowed. Recipients may use PAP:GREEN information to ping the target, block incoming/outgoing traffic from/to the target or specifically configure honeypots to interact with the target.

WHITE

PAP:WHITE

(PAP:WHITE) No restrictions in using this information.

accessnow

accessnow namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Access Now

anti-corruption-transparency

The organization campaigns, or takes other actions against corruption and transparency.

accessnow:anti-corruption-transparency

Anti-Corruption and transparency

The organization campaigns, or takes other actions against corruption and transparency.

anti-war-violence

The organization campaigns, or takes other actions against war

accessnow:anti-war-violence

Anti-War / Anti-Violence

The organization campaigns, or takes other actions against war

culture

The organization campaigns or acts to promote cultural events

accessnow:culture

Culture

The organization campaigns or acts to promote cultural events

economic-change

Issues of economic policy, wealth distribution, etc.

accessnow:economic-change

Economic Change

Issues of economic policy, wealth distribution, etc.

education

The organization is concerned with some form of education

accessnow:education

Education

The organization is concerned with some form of education

election-monitoring

The organization is an election monitor, or involved in election monitoring

accessnow:election-monitoring

Election Monitoring

The organization is an election monitor, or involved in election monitoring

environment

The organization campaigns or acts to protect the environment

accessnow:environment

Environment

The organization campaigns or acts to protect the environment

freedom-expression

The organization is concerned with freedom of speech issues

accessnow:freedom-expression

Freedom of Expression

The organization is concerned with freedom of speech issues

freedom-tool-development

The organization develops tools for use in defending or extending digital rights

accessnow:freedom-tool-development

Freedom Tool Development

The organization develops tools for use in defending or extending digital rights

funding

```
The organization is a funder of organizations or projects working with at risk users
```

accessnow:funding

Funding

```
The organization is a funder of organizations or projects working with at risk users
```

health

The organization prevents epidemic illness or acts on curing them

accessnow:health

Health Issues

The organization prevents epidemic illness or acts on curing them

human-rights

relating to the detection, recording, exposure, or challenging of abuses of human rights

accessnow:human-rights

Human Rights Issues

relating to the detection, recording, exposure, or challenging of abuses of human rights

internet-telecom

Issues of digital rights in electronic communications

accessnow:internet-telecom

Internet and Telecoms

Issues of digital rights in electronic communications

lgbt-gender-sexuality

Issues relating to the Lesbian, Gay, Bi, Transgender community

accessnow:lgbt-gender-sexuality

LGBT / Gender / Sexuality

Issues relating to the Lesbian, Gay, Bi, Transgender community

policy

The organization is a policy think-tank, or policy advocate

accessnow:policy

Policy

The organization is a policy think-tank, or policy advocate

politics

The organization takes a strong political view or is a political entity

accessnow:politics

Politics

The organization takes a strong political view or is a political entity

privacy

Issues relating to the individual’s reasonable right to privacy

accessnow:privacy

Privacy

Issues relating to the individual’s reasonable right to privacy

rapid-response

The organization provides rapid response type capability for civil society

accessnow:rapid-response

Rapid Response

The organization provides rapid response type capability for civil society

refugees

Issues relating to displaced people

accessnow:refugees

Refugees

Issues relating to displaced people

security

Issues relating to physical or information security

accessnow:security

Security

Issues relating to physical or information security

womens-right

Issues pertaining to inequality between men and women, or issues of particular relevance to women

accessnow:womens-right

Women's Rights

Issues pertaining to inequality between men and women, or issues of particular relevance to women

youth-rights

Issues of particular relevance to youth

accessnow:youth-rights

Youth Rights

Issues of particular relevance to youth

action-taken

action-taken namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Action taken

informed ISP/Hosting Service Provider

action-taken:informed ISP/Hosting Service Provider

Informed ISP/Hosting Service Provider

informed Registrar

action-taken:informed Registrar

Informed Registrar

informed Registrant

action-taken:informed Registrant

Informed Registrant

informed abuse-contact (domain)

action-taken:informed abuse-contact (domain)

Informed abuse-contact (domain)

informed abuse-contact (IP)

action-taken:informed abuse-contact (IP)

Informed abuse-contact (IP)

informed legal department

action-taken:informed legal department

Informed legal department

admiralty-scale

admiralty-scale namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

The Admiralty Scale (also called the NATO System) is used to rank the reliability of a source and the credibility of an information.

source-reliability

admiralty-scale:source-reliability="a"

Completely reliable

Associated numerical value="100"

admiralty-scale:source-reliability="b"

Usually reliable

Associated numerical value="75"

admiralty-scale:source-reliability="c"

Fairly reliable

Associated numerical value="50"

admiralty-scale:source-reliability="d"

Not usually reliable

Associated numerical value="25"

admiralty-scale:source-reliability="e"

Unreliable

admiralty-scale:source-reliability="f"

Reliability cannot be judged

information-credibility

admiralty-scale:information-credibility="1"

Confirmed by other sources

Associated numerical value="100"

admiralty-scale:information-credibility="2"

Probably true

Associated numerical value="75"

admiralty-scale:information-credibility="3"

Possibly true

Associated numerical value="50"

admiralty-scale:information-credibility="4"

Doubtful

Associated numerical value="25"

admiralty-scale:information-credibility="5"

Improbable

admiralty-scale:information-credibility="6"

Truth cannot be judged

adversary

adversary namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

An overview and description of the adversary infrastructure

infrastructure-status

adversary:infrastructure-status="unknown"

Infrastructure ownership and status is unknown

adversary:infrastructure-status="compromised"

Infrastructure compromised by or in the benefit of the adversary

adversary:infrastructure-status="own-and-operated"

Infrastructure own and operated by the adversary

infrastructure-action

adversary:infrastructure-action="passive-only"

Only passive requests shall be performed to avoid detection by the adversary

adversary:infrastructure-action="take-down"

Take down requests can be performed in order to deactivate the adversary infrastructure

adversary:infrastructure-action="monitoring-active"

Monitoring requests are ongoing on the adversary infrastructure

adversary:infrastructure-action="pending-law-enforcement-request"

Law enforcement requests are ongoing on the adversary infrastructure

infrastructure-state

adversary:infrastructure-state="unknown"

Infrastructure state is unknown or cannot be evaluated

adversary:infrastructure-state="active"

Infrastructure state is active and actively used by the adversary

adversary:infrastructure-state="down"

Infrastructure state is known to be down

infrastructure-type

adversary:infrastructure-type="unknown"

Infrastructure usage by the adversary is unknown

adversary:infrastructure-type="proxy"

Infrastructure used as proxy between the target and the adversary

adversary:infrastructure-type="drop-zone"

Infrastructure used by the adversary to store information related to his campaigns

adversary:infrastructure-type="exploit-distribution-point"

Infrastructure used to distribute exploit towards target(s)

adversary:infrastructure-type="vpn"

Infrastructure used by the adversary as Virtual Private Network to hide activities and reduce the traffic analysis surface

adversary:infrastructure-type="panel"

Panel used by the adversary to control or maintain his infrastructure

adversary:infrastructure-type="tds"

Traffic Distribution Systems including exploit delivery or/and web monetization channels

ais-marking

ais-marking namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

The AIS Marking Schema implementation is maintained by the National Cybersecurity and Communication Integration Center (NCCIC) of the U.S. Department of Homeland Security (DHS)

TLPMarking

ais-marking:TLPMarking="WHITE"

WHITE

ais-marking:TLPMarking="GREEN"

GREEN

ais-marking:TLPMarking="AMBER"

AMBER

AISConsent

ais-marking:AISConsent="EVERYONE"

EVERYONE

ais-marking:AISConsent="USG"

USG

ais-marking:AISConsent="NONE"

NONE

CISA_Proprietary

ais-marking:CISA_Proprietary="true"

true

ais-marking:CISA_Proprietary="false"

false

AISMarking

ais-marking:AISMarking="Is_Proprietary"

Is_Proprietary

ais-marking:AISMarking="Not_Proprietary"

Not_Proprietary

analyst-assessment

analyst-assessment namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

A series of assessment predicates describing the analyst capabilities to perform analysis. These assessment can be assigned by the analyst him/herself or by another party evaluating the analyst.

experience

The analyst experience expressed in years range in the field tagged. The year range is based on a standard 40-hour work week.

analyst-assessment:experience="less-than-1-year"

Less than 1 year

Associated numerical value="1"

analyst-assessment:experience="between-1-and-5-years"

Between 1 and 5 years

Associated numerical value="2"

analyst-assessment:experience="between-5-and-10-years"

Between 5 and 10 years

Associated numerical value="3"

analyst-assessment:experience="between-10-and-20-years"

Between 10 and 20 years

Associated numerical value="4"

analyst-assessment:experience="more-than-20-years"

More than 20 years

Associated numerical value="5"

binary-reversing-arch

Architecture that the analyst has experience with.

analyst-assessment:binary-reversing-arch="x86"

x86-32 & x86-64

analyst-assessment:binary-reversing-arch="arm"

ARM & ARM-64

analyst-assessment:binary-reversing-arch="mips"

mips & mips-64

analyst-assessment:binary-reversing-arch="powerpc"

PowerPC

binary-reversing-experience

The analyst experience in reversing expressed in years range in the field tagged. The year range is based on a standard 40-hour work week.

analyst-assessment:binary-reversing-experience="less-than-1-year"

Less than 1 year

Associated numerical value="1"

analyst-assessment:binary-reversing-experience="between-1-and-5-years"

Between 1 and 5 years

Associated numerical value="2"

analyst-assessment:binary-reversing-experience="between-5-and-10-years"

Between 5 and 10 years

Associated numerical value="3"

analyst-assessment:binary-reversing-experience="between-10-and-20-years"

Between 10 and 20 years

Associated numerical value="4"

analyst-assessment:binary-reversing-experience="more-than-20-years"

More than 20 years

Associated numerical value="5"

os

Operating System that the analyst has experience with.

analyst-assessment:os="windows"

Current Microsoft Windows system

analyst-assessment:os="linux"

GNU/linux derivative OS

analyst-assessment:os="ios"

Current IOS

analyst-assessment:os="macos"

Current Apple OS

analyst-assessment:os="android"

Current Android OS

analyst-assessment:os="bsd"

BSD

web

Web application vulnerabilities and technique that the analyst has experience with.

analyst-assessment:web="ipex"

Inter-protocol exploitations

analyst-assessment:web="common"

Common vulnerabilities as SQL injections, CSRF, XSS, CSP bypasses, etc.

analyst-assessment:web="js-desobfuscation"

De-obfuscation of Javascript payloads

web-experience

The analyst experience expressed to web application security in years range in the field tagged.

analyst-assessment:web-experience="less-than-1-year"

Less than 1 year

Associated numerical value="1"

analyst-assessment:web-experience="between-1-and-5-years"

Between 1 and 5 years

Associated numerical value="2"

analyst-assessment:web-experience="between-5-and-10-years"

Between 5 and 10 years

Associated numerical value="3"

analyst-assessment:web-experience="between-10-and-20-years"

Between 10 and 20 years

Associated numerical value="4"

analyst-assessment:web-experience="more-than-20-years"

More than 20 years

Associated numerical value="5"

crypto-experience

The analyst experience related to cryptography expressed in years range in the field tagged.

analyst-assessment:crypto-experience="less-than-1-year"

Less than 1 year

Associated numerical value="1"

analyst-assessment:crypto-experience="between-1-and-5-years"

Between 1 and 5 years

Associated numerical value="2"

analyst-assessment:crypto-experience="between-5-and-10-years"

Between 5 and 10 years

Associated numerical value="3"

analyst-assessment:crypto-experience="between-10-and-20-years"

Between 10 and 20 years

Associated numerical value="4"

analyst-assessment:crypto-experience="more-than-20-years"

More than 20 years

Associated numerical value="5"

binary-class

binary-class namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Custom taxonomy for types of binary file.

type

binary-class:type="good"

Known Good/Safe

binary-class:type="malicious"

Known Bad/Malicious

binary-class:type="unknown"

Not yet known

circl

circl namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

CIRCL Taxonomy - Schemes of Classification in Incident Response and Detection

incident-classification

circl:incident-classification="spam"

Spam

circl:incident-classification="system-compromise"

System compromise

circl:incident-classification="scan"

Scan

circl:incident-classification="denial-of-service"

Denial of Service

circl:incident-classification="copyright-issue"

Copyright issue

circl:incident-classification="phishing"

Phishing

circl:incident-classification="malware"

Malware

circl:incident-classification="XSS"

XSS

circl:incident-classification="vulnerability"

Vulnerability

circl:incident-classification="fastflux"

Fastflux

circl:incident-classification="sql-injection"

SQL Injection

circl:incident-classification="information-leak"

Information leak

circl:incident-classification="scam"

Scam

circl:incident-classification="cryptojacking"

Cryptojacking

topic

circl:topic="finance"

Finance

circl:topic="ict"

ICT

circl:topic="individual"

Individual

circl:topic="industry"

Industry

circl:topic="medical"

Medical

circl:topic="services"

Services

circl:topic="undefined"

Undefined

collaborative-intelligence

collaborative-intelligence namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Collaborative intelligence support language is a common language to support analysts to perform their analysis to get crowdsourced support when using threat intelligence sharing platform like MISP. The objective of this language is to advance collaborative analysis and to share earlier than later.

request

Request predicate covers all the requests which can be done by analysts or organisations willing to get additional information to support their analysis.

collaborative-intelligence:request="sample"

Request a binary sample

collaborative-intelligence:request="deobfuscated-sample"

Request a deobfuscated sample of the shared sample

collaborative-intelligence:request="more-samples"

Request additional samples compared to the original analysis to build a competitive analysis on the reversing aspect

collaborative-intelligence:request="related-samples"

Request related samples required for further analysis

collaborative-intelligence:request="static-analysis"

Request additional static analysis or reversing on the information shared

collaborative-intelligence:request="detection-signature"

Request detection signature from

collaborative-intelligence:request="context"

Request more contextual information

collaborative-intelligence:request="abuse-contact"

Request an abuse contact to report to

collaborative-intelligence:request="historical-information"

Request more historical information from

collaborative-intelligence:request="complementary-validation"

Request complementary validation

collaborative-intelligence:request="target-information"

Request about the target(s) including field of activities or companies

collaborative-intelligence:request="request-analysis"

Request further technical or tactical analysis

collaborative-intelligence:request="more-information"

Request for generic additional information

csirt_case_classification

csirt_case_classification namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

It is critical that the CSIRT provide consistent and timely response to the customer, and that sensitive information is handled appropriately. This document provides the guidelines needed for CSIRT Incident Managers (IM) to classify the case category, criticality level, and sensitivity level for each CSIRT case. This information will be entered into the Incident Tracking System (ITS) when a case is created. Consistent case classification is required for the CSIRT to provide accurate reporting to management on a regular basis. In addition, the classifications will provide CSIRT IM's with proper case handling procedures and will form the basis of SLA's between the CSIRT and other Company departments.

incident-category

csirt_case_classification:incident-category="DOS"

Denial of service / Distributed Denial of service

csirt_case_classification:incident-category="forensics"

Forensics work

csirt_case_classification:incident-category="compromised-information"

Attempted or successful destruction, corruption, or disclosure of sensitive corporate information or Intellectual Property

csirt_case_classification:incident-category="compromised-asset"

Compromised host (root account, Trojan, rootkit), network device, application, user account.

csirt_case_classification:incident-category="unlawful-activity"

Theft / Fraud / Human Safety / Child Porn

csirt_case_classification:incident-category="internal-hacking"

Reconnaissance or Suspicious activity originating from inside the Company corporate network, excluding malware

csirt_case_classification:incident-category="external-hacking"

Reconnaissance or Suspicious Activity originating from outside the Company corporate network (partner network, Internet), excluding malware.

csirt_case_classification:incident-category="malware"

A virus or worm typically affecting multiple corporate devices. This does not include compromised hosts that are being actively controlled by an attacker via a backdoor or Trojan.

csirt_case_classification:incident-category="email"

Spoofed email, SPAM, and other email security-related events.

csirt_case_classification:incident-category="consulting"

Security consulting unrelated to any confirmed incident

csirt_case_classification:incident-category="policy-violation"

Violation of various policies

criticality-classification

csirt_case_classification:criticality-classification="1"

Incident affecting critical systems or information with potential to be revenue or customer impacting.

csirt_case_classification:criticality-classification="2"

Incident affecting non-critical systems or information, not revenue or customer impacting. Employee investigations that are time sensitive should typically be classified at this level.

csirt_case_classification:criticality-classification="3"

Possible incident, non-critical systems. Incident or employee investigations that are not time sensitive. Long-term investigations involving extensive research and/or detailed forensic work.

sensitivity-classification

csirt_case_classification:sensitivity-classification="1"

Extremely Sensitive

csirt_case_classification:sensitivity-classification="2"

Sensitive

csirt_case_classification:sensitivity-classification="3"

Not Sensitive

cssa

cssa namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

The CSSA agreed sharing taxonomy.

sharing-class

cssa:sharing-class="high_profile"

Generated within the company during incident/case related investigations or forensic analysis or via malware reversing, validated by humans and highly contextualized.

cssa:sharing-class="vetted"

Generated within the company, validated by a human prior to sharing, data points have been contextualized (to a degree) e.g. IPs are related to C2 or drop site.

cssa:sharing-class="unvetted"

Generated within the company by automated means without human interaction e.g., by malware sandbox, honeypots, IDS, etc.

origin

cssa:origin="manual_investigation"

Information gathered by an analyst/incident responder/forensic expert/etc.

cssa:origin="honeypot"

Information coming out of honeypots.

cssa:origin="sandbox"

Information coming out of sandboxes.

cssa:origin="email"

Information coming out of email infrastructure.

cssa:origin="3rd-party"

Information from outside the company.

cssa:origin="other"

If none of the other origins applies.

cssa:origin="unknown"

Origin of the data unknown.

analyse

cyber-threat-framework

cyber-threat-framework namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Cyber Threat Framework was developed by the US Government to enable consistent characterization and categorization of cyber threat events, and to identify trends or changes in the activities of cyber adversaries. https://www.dni.gov/index.php/cyber-threat-framework

Preparation

cyber-threat-framework:Preparation="plan-activity"

Plan activity

Associated numerical value="10"

cyber-threat-framework:Preparation="conduct-research-and-analysis"

Conduct research & analysis

Associated numerical value="11"

cyber-threat-framework:Preparation="develop-resource-and-capabilities"

Develop resources & capabilities

Associated numerical value="12"

cyber-threat-framework:Preparation="acquire-victim-and-specific-knowledge"

Acquire victim & specific knowledge

Associated numerical value="13"

cyber-threat-framework:Preparation="complete-preparations"

Complete preparations

Associated numerical value="14"

Engagement

cyber-threat-framework:Engagement="deploy-capability"

Deploy capability

Associated numerical value="20"

cyber-threat-framework:Engagement="interact-with-intended-victim"

Interact with intended victim

Associated numerical value="21"

cyber-threat-framework:Engagement="exploit-vulnerabilities"

Exploit vulnerabilities

Associated numerical value="22"

cyber-threat-framework:Engagement="deliver-malicious-capabilities"

Deliver malicious capabilities

Associated numerical value="23"

Presence

cyber-threat-framework:Presence="establish-controlled-access"

Establish controlled access

Associated numerical value="30"

cyber-threat-framework:Presence="hide"

Hide

Associated numerical value="31"

cyber-threat-framework:Presence="expand-presence"

Expand presence

Associated numerical value="32"

cyber-threat-framework:Presence="refine-focus-of-activity"

Refine focus of activity

Associated numerical value="33"

cyber-threat-framework:Presence="establish-persistence"

Establish persistence

Associated numerical value="34"

Effect/Consequence

cyber-threat-framework:Effect/Consequence="enable-other-operations"

Enable other operations

Associated numerical value="40"

cyber-threat-framework:Effect/Consequence="deny-access"

Deny access

Associated numerical value="41"

cyber-threat-framework:Effect/Consequence="extract-data"

Extract data

Associated numerical value="42"

cyber-threat-framework:Effect/Consequence="alter-data-and-or-computer-network-or-system-behavior"

Alter data and/or computer, network or system behavior

Associated numerical value="43"

cyber-threat-framework:Effect/Consequence="destroy-hardware-software-or-data"

Destroy HW/SW/data

Associated numerical value="44"

ddos

ddos namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

```
Distributed Denial of Service - or short: DDoS - taxonomy supports the description of
Denial of Service attacks and especially the types they belong too.
```

type

Types and techniques described the way that the attack is performed to launch the Denial of Service attacks. A combination of type values can be used to explain combined techniques and methods.

ddos:type="amplification-attack"

Amplification attack

ddos:type="reflected-spoofed-attack"

Reflected and Spoofed attack

ddos:type="slow-read-attack"

Slow Read attack

ddos:type="flooding-attack"

Flooding attack

ddos:type="post-attack"

Large POST HTTP attack

de-vs

de-vs namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

German (DE) Government classification markings (VS).

Einstufung

de-vs:Einstufung="STRENG GEHEIM"

STRENG GEHEIM

Kenntnisnahme durch Unbefugte kann den Bestand oder lebenswichtige Interessen der Bundesrepublik Deutschland oder eines ihrer Länder gefährden.

de-vs:Einstufung="GEHEIM"

GEHEIM

Kenntnisnahme durch Unbefugte kann die Sicherheit der Bundesrepublik Deutschland oder eines ihrer Länder gefährden oder ihren Interessen schweren Schaden zufügen.

de-vs:Einstufung="VS-VERTRAULICH"

VS-VERTRAULICH

Kenntnisnahme durch Unbefugte kann für die Interessen der Bundesrepublik Deutschland oder

eines ihrer Länder schädlich sein.

de-vs:Einstufung="VS-NfD"

VS-NUR FÜR DEN DIENSTGEBRAUCH

Kenntnisnahme durch Unbefugte kann für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder nachteilig sein.

Schutzwort

de-vs:Schutzwort="Dummy"

Dummy

Platzhalter.

dhs-ciip-sectors

dhs-ciip-sectors namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

DHS critical sectors as in https://www.dhs.gov/critical-infrastructure-sectors

DHS-critical-sectors

dhs-ciip-sectors:DHS-critical-sectors="chemical"

Chemical

dhs-ciip-sectors:DHS-critical-sectors="commercial-facilities"

Commercial Facilities

dhs-ciip-sectors:DHS-critical-sectors="communications"

Communications

dhs-ciip-sectors:DHS-critical-sectors="critical-manufacturing"

Critical Manufacturing

dhs-ciip-sectors:DHS-critical-sectors="dams"

Dams

dhs-ciip-sectors:DHS-critical-sectors="dib"

Defense Industrial Base

dhs-ciip-sectors:DHS-critical-sectors="emergency-services"

Emergency services

dhs-ciip-sectors:DHS-critical-sectors="energy"

energy

dhs-ciip-sectors:DHS-critical-sectors="financial-services"

Financial Services

dhs-ciip-sectors:DHS-critical-sectors="food-agriculture"

Food and Agriculture

dhs-ciip-sectors:DHS-critical-sectors="government-facilities"

Government Facilities

dhs-ciip-sectors:DHS-critical-sectors="healthcare-public"

Healthcare and Public Health

dhs-ciip-sectors:DHS-critical-sectors="it"

Information Technology

dhs-ciip-sectors:DHS-critical-sectors="nuclear"

Nuclear

dhs-ciip-sectors:DHS-critical-sectors="transport"

Transportation Systems

dhs-ciip-sectors:DHS-critical-sectors="water"

Water and water systems

sector

diamond-model

diamond-model namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

The Diamond Model for Intrusion Analysis, a phase-based model developed by Lockheed Martin, aims to help categorise and identify the stage of an attack.

Adversary

diamond-model:Adversary

An adversary is the actor/organization responsible for utilizing a capability against the victim to achieve their intent.

Capability

diamond-model:Capability

The capability describes the tools and/or techniques of the adversary used in the event. It includes all means to affect the victim from the most manual “unsophisticated” methods (e.g., manual password guessing) to the most sophisticated automated techniques.

Infrastructure

diamond-model:Infrastructure

The infrastructure feature describes the physical and/or logical communication structures the adversary uses to deliver a capability, maintain control of capabilities (e.g., commandand-control/C2), and effect results from the victim (e.g., exfiltrate data). As with the other features, the infrastructure can be as specific or broad as necessary. Examples include: Internet Protocol (IP) addresses, domain names, e-mail addresses, Morse code flashes from a phone’s voice-mail light watched from across a street, USB devices found in a parking lot and inserted into a workstation, or the compromising emanations from hardware (e.g., Van Eck Phreaking) being collected by a nearby listening post.

Victim

diamond-model:Victim

A victim is the target of the adversary and against whom vulnerabilities and exposures are exploited and capabilities used. A victim can be described in whichever way necessary and appropriate: organization, person, target email address, IP address, domain, etc. However, it is useful to define the victim persona and their assets separately as they serve different analytic

functions. Victim personae are useful in non-technical analysis such as cyber-victimology and social-political centered approaches whereas victim assets are associated with common technical approaches such as vulnerability analysis..

dni-ism

dni-ism namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

A subset of Information Security Marking Metadata ISM as required by Executive Order (EO) 13526. As described by DNI.gov as Data Encoding Specifications for Information Security Marking Metadata in Controlled Vocabulary Enumeration Values for ISM

classification:all

dni-ism:classification:all="R"

RESTRICTED

dni-ism:classification:all="C"

CONFIDENTIAL

dni-ism:classification:all="S"

SECRET

dni-ism:classification:all="TS"

TOP SECRET

dni-ism:classification:all="U"

UNCLASSIFIED

classification:us

dni-ism:classification:us="C"

CONFIDENTIAL

dni-ism:classification:us="S"

SECRET

dni-ism:classification:us="TS"

TOP SECRET

dni-ism:classification:us="U"

UNCLASSIFIED

scicontrols

dni-ism:scicontrols="EL"

ENDSEAL

dni-ism:scicontrols="EL-EU"

ECRU

dni-ism:scicontrols="EL-NK"

NONBOOK

dni-ism:scicontrols="HCS"

HCS

dni-ism:scicontrols="HCS-O"

HCS-O

dni-ism:scicontrols="HCS-P"

HCS-P

dni-ism:scicontrols="KDK"

KLONDIKE

dni-ism:scicontrols="KDK-BLFH"

KDK BLUEFISH

dni-ism:scicontrols="KDK-IDIT"

KDK IDITAROD

dni-ism:scicontrols="KDK-KAND"

KDK KANDIK

dni-ism:scicontrols="RSV"

RESERVE

dni-ism:scicontrols="SI"

SPECIAL INTELLIGENCE

dni-ism:scicontrols="SI-G"

SI-GAMMA

dni-ism:scicontrols="TK"

TALENT KEYHOLE

complies:with

dni-ism:complies:with="USGov"

Document claims compliance with all rules encoded in ISM for documents produced by the US Federal Government. This is the minimum set of rules for US documents to adhere to, and all US documents should claim compliance with USGov.

dni-ism:complies:with="USIC"

Document claims compliance with all rules encoded in ISM for documents produced by the US Intelligence Community. Documents that claim compliance with USIC MUST also claim compliance with USGov.

dni-ism:complies:with="USDOD"

Document claims compliance with all rules encoded in ISM for documents produced by the US Department of Defense. Documents that claim compliance with USDOD MUST also claim compliance with USGov.

dni-ism:complies:with="OtherAuthority"

Document claims compliance with an authority other than the USGov, USIC, or USDOD.

atomicenergymarkings

dni-ism:atomicenergymarkings="RD"

RESTRICTED DATA

dni-ism:atomicenergymarkings="RD-CNWDI"

RD-CRITICAL NUCLEAR WEAPON DESIGN INFORMATION

dni-ism:atomicenergymarkings="FRD"

FORMERLY RESTRICTED DATA

dni-ism:atomicenergymarkings="DCNI"

DoD CONTROLLED NUCLEAR INFORMATION

dni-ism:atomicenergymarkings="UCNI"

DoE CONTROLLED NUCLEAR INFORMATION

dni-ism:atomicenergymarkings="TFNI"

TRANSCLASSIFIED FOREIGN NUCLEAR INFORMATION

notice

dni-ism:notice="FISA"

FISA Warning statement

dni-ism:notice="IMC"

IMCON Warning statement

dni-ism:notice="CNWDI"

Controled Nuclear Weapon Design Information Warning statement

dni-ism:notice="RD"

RD Warning statement

dni-ism:notice="FRD"

FRD Warning statement

dni-ism:notice="DS"

LIMDIS caveat

dni-ism:notice="LES"

LES Notice

dni-ism:notice="LES-NF"

LES-NF Notice

dni-ism:notice="DSEN"

DSEN Notice

dni-ism:notice="DoD-Dist-A"

DoD Distribution statement A from DoD Directive 5230.24

dni-ism:notice="DoD-Dist-B"

DoD Distribution statement B from DoD Directive 5230.24

dni-ism:notice="DoD-Dist-C"

DoD Distribution statement C from DoD Directive 5230.24

dni-ism:notice="DoD-Dist-D"

DoD Distribution statement D from DoD Directive 5230.24

dni-ism:notice="DoD-Dist-E"

DoD Distribution statement E from DoD Directive 5230.24

dni-ism:notice="DoD-Dist-F"

DoD Distribution statement F from DoD Directive 5230.24

dni-ism:notice="DoD-Dist-X"

DoD Distribution statement X from DoD Directive 5230.24

dni-ism:notice="US-Person"

US Person info Notice

dni-ism:notice="pre13526ORCON"

Indicates that an instance document must abide by rules pertaining to ORIGINATOR CONTROLLED data issued prior to Executive Order 13526.

dni-ism:notice="POC"

Indicates that the contents of this notice specify the contact information for a required point-of-contact.

dni-ism:notice="COMSEC"

COMSEC Notice

nonic

dni-ism:nonic="NNPI"

NAVAL NUCLEAR PROPULSION INFORMATION

dni-ism:nonic="DS"

LIMITED DISTRIBUTION

dni-ism:nonic="XD"

EXCLUSIVE DISTRIBUTION

dni-ism:nonic="ND"

NO DISTRIBUTION

dni-ism:nonic="SBU"

SENSITIVE BUT UNCLASSIFIED

dni-ism:nonic="SBU-NF"

SENSITIVE BUT UNCLASSIFIED NOFORN

dni-ism:nonic="LES"

LAW ENFORCEMENT SENSITIVE

dni-ism:nonic="LES-NF"

LAW ENFORCEMENT SENSITIVE NOFORN

dni-ism:nonic="SSI"

SENSITIVE SECURITY INFORMATION

nonuscontrols

dni-ism:nonuscontrols="ATOMAL"

NATO Atomal mark

dni-ism:nonuscontrols="BOHEMIA"

NATO Bohemia mark

dni-ism:nonuscontrols="BALK"

NATO Balk mark

dissem

dni-ism:dissem="RS"

RISK SENSITIVE

dni-ism:dissem="FOUO"

FOR OFFICIAL USE ONLY

dni-ism:dissem="OC"

ORIGINATOR CONTROLLED

dni-ism:dissem="OC-USGOV"

ORIGINATOR CONTROLLED US GOVERNMENT

dni-ism:dissem="IMC"

CONTROLLED IMAGERY

dni-ism:dissem="NF"

NOT RELEASABLE TO FOREIGN NATIONALS

dni-ism:dissem="PR"

CAUTION-PROPRIETARY INFORMATION INVOLVED

dni-ism:dissem="REL"

AUTHORIZED FOR RELEASE TO

dni-ism:dissem="RELIDO"

RELEASABLE BY INFORMATION DISCLOSURE OFFICIAL

dni-ism:dissem="DSEN"

DEA SENSITIVE

dni-ism:dissem="FISA"

FOREIGN INTELLIGENCE SURVEILLANCE ACT

dni-ism:dissem="DISPLAYONLY"

AUTHORIZED FOR DISPLAY BUT NOT RELEASE TO

domain-abuse

domain-abuse namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Domain Name Abuse - taxonomy to tag domain names used for cybercrime. Use europol-incident to tag abuse-activity

domain-status

Domain status - describes the registration status of the domain name

domain-abuse:domain-status="active"

Registered & active

Domain name is registered and DNS is delegated

domain-abuse:domain-status="inactive"

Registered & inactive

Domain name is registered and DNS is not delegated

domain-abuse:domain-status="suspended"

Registered & suspended

Domain name is registered & DNS delegation is temporarily removed by the registry

domain-abuse:domain-status="not-registered"

Not registered

Domain name is not registered and open for registration

domain-abuse:domain-status="not-registrable"

Not registrable

Domain is not registered and cannot be registered

domain-abuse:domain-status="grace-period"

Grace period

Domain is deleted and still reserved for previous owner

domain-access-method

Domain Access - describes how the adversary has gained access to the domain name

domain-abuse:domain-access-method="criminal-registration"

Criminal registration

Domain name is registered for criminal purposes

domain-abuse:domain-access-method="compromised-webserver"

Compromised webserver

Webserver is compromised for criminal purposes

domain-abuse:domain-access-method="compromised-dns"

Compromised DNS

Compromised authoritative DNS or compromised delegation

domain-abuse:domain-access-method="sinkhole"

Sinkhole

Domain Name is sinkholed for research, detection, LE

ecsirt

ecsirt namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Incident Classification by the ecsirt.net version mkVI of 31 March 2015 enriched with IntelMQ taxonomy-type mapping.

abusive-content

Abusive Content.

ecsirt:abusive-content="spam"

spam

Or 'Unsolicited Bulk Email', this means that the recipient has not granted verifiable permission for the message to be sent and that the message is sent as part of a larger collection of messages, all having a functionally comparable content.

ecsirt:abusive-content="harmful-speech"

Harmful Speech

Discreditation or discrimination of somebody e.g. cyber stalking, racism and threats against one or more individuals).

ecsirt:abusive-content="violence"

Child/Sexual/Violence/...

Child Pornography, glorification of violence, ...

malicious-code

Software that is intentionally included or inserted in a system for a harmful purpose. A user interaction is normally necessary to activate the code.

ecsirt:malicious-code="virus"

Virus

ecsirt:malicious-code="worm"

Worm

ecsirt:malicious-code="trojan"

Trojan

ecsirt:malicious-code="spyware"

Spyware

ecsirt:malicious-code="dialer"

Dialer

ecsirt:malicious-code="rootkit"

Rootkit

ecsirt:malicious-code="malware"

Malware

ecsirt:malicious-code="botnet-drone"

Botnet drone

ecsirt:malicious-code="ransomware"

Ransomware

ecsirt:malicious-code="malware-configuration"

Malware configuration

ecsirt:malicious-code="c&c"

C&C

information-gathering

Information Gathering.

ecsirt:information-gathering="scanner"

Scanning

Attacks that send requests to a system to discover weak points. This includes also some kind of testing processes to gather information about hosts, services and accounts. Examples: fingerd, DNS querying, ICMP, SMTP (EXPN, RCPT, ...), port scanning.

ecsirt:information-gathering="sniffing"

Sniffing

Observing and recording of network traffic (wiretapping).

ecsirt:information-gathering="social-engineering"

Social Engineering

Gathering information from a human being in a non-technical way (e.g. lies, tricks, bribes, or threats).

intrusion-attempts

Intrusion Attempts.

ecsirt:intrusion-attempts="ids-alert"

Exploiting of known Vulnerabilities

An attempt to compromise a system or to disrupt any service by exploiting vunerabilities with a standardised identifier such as CVE name (e.g. buffer overflow, backdoor, cross site scripting, etc.)

ecsirt:intrusion-attempts="brute-force"

Login attempts

Multiple login attempts (Guessing / cracking of passwords, brute force).

ecsirt:intrusion-attempts="exploit"

New attack signature

An attempt using an unknown exploit.

intrusions

A successful compromise of a system or application (service). This can have been caused remotely by a known or new vulnerability, but also by an unauthorized local access. Also includes being part of a botnet.

ecsirt:intrusions="privileged-account-compromise"

Privileged Account Compromise

ecsirt:intrusions="unprivileged-account-compromise"

Unprivileged Account Compromise

ecsirt:intrusions="application-compromise"

Application Compromise

ecsirt:intrusions="bot"

Bot

ecsirt:intrusions="defacement"

defacement

ecsirt:intrusions="compromised"

compromised

ecsirt:intrusions="backdoor"

backdoor

availability

By this kind of an attack a system is bombarded with so many packets that the operations are delayed or the system crashes. DoS examples are ICMP and SYN floods, Teardrop attacks and mail-bombing. DDoS often is based on DoS attacks originating from botnets, but also other scenarios exist like DNS Amplification attacks. However, the availability also can be affected by local actions (destruction, disruption of power supply, etc.) – or by Act of God, spontaneous failures or human error, without malice or gross neglect being involved.

ecsirt:availability="dos"

DoS

Denial of Service.

ecsirt:availability="ddos"

DDoS

Distributed Denial of Service.

ecsirt:availability="sabotage"

Sabotage

Sabotage.

ecsirt:availability="outage"

Outage (no malice)

Outage (no malice).

information-content-security

Besides a local abuse of data and systems the information security can be endangered by a successful account or application compromise. Furthermore attacks are possible that intercept and access information during transmission (wiretapping, spoofing or hijacking). Human/configuration/software error can also be the cause.

ecsirt:information-content-security="Unauthorised-information-access"

Unauthorised access to information

ecsirt:information-content-security="Unauthorised-information-modification"

Unauthorised modification of information

ecsirt:information-content-security="dropzone"

dropzone

fraud

Fraud.

ecsirt:fraud="unauthorized-use-of-resources"

Unauthorized use of resources

Using resources for unauthorized purposes including profit-making ventures (E.g. the use of e-mail to participate in illegal profit chain letters or pyramid schemes).

ecsirt:fraud="copyright"

Copyright

Offering or Installing copies of unlicensed commercial software or other copyright protected materials (Warez).

ecsirt:fraud="masquerade"

Masquerade

Type of attacks in which one entity illegitimately assumes the identity of another in order to benefit

from it.

ecsirt:fraud="phishing"

Phishing

Masquerading as another entity in order to persuade the user to reveal a private credential.

vulnerable

Open resolvers, world readable printers, vulnerability apparent from Nessus etc scans, virus signatures not up-to-date, etc

ecsirt:vulnerable="vulnerable-service"

Open for abuse

other

All incidents which don't fit in one of the given categories should be put into this class. If the number of incidents in this category increases, it is an indicator that the classification scheme must be revised

ecsirt:other="blacklist"

blacklist

ecsirt:other="unknown"

unknown

ecsirt:other="other"

other

test

Meant for testing.

ecsirt:test="test"

Test

enisa

enisa namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

The present threat taxonomy is an initial version that has been developed on the basis of available ENISA material. This material has been used as an ENISA-internal structuring aid for information collection and threat consolidation purposes. It emerged in the time period 2012-2015.

physical-attack

Threats of intentional, hostile human actions.

enisa:physical-attack="fraud"

Fraud

Fraud committed by humans.

enisa:physical-attack="fraud-by-employees"

Fraud committed by employees

Fraud committed by employees or others that are in relation with entities, who have access to entities' information and IT assets.

enisa:physical-attack="sabotage"

Sabotage

Intentional actions (non-fulfilment or defective fulfilment of personal duties) aimed to cause disruption or damage to IT assets.

enisa:physical-attack="vandalism"

Vandalism

Act of physically damaging IT assets.

enisa:physical-attack="theft"

Theft (of devices, storage media and documents)

Stealing information or IT assets. Robbery.

enisa:physical-attack="theft-of-mobile-devices"

Theft of mobile devices (smartphones/ tablets)

Taking away another person’s property in the form of mobile devices, for example smartphones, tablets.

enisa:physical-attack="theft-of-fixed-hardware"

Theft of fixed hardware

Taking away another person’s hardware property (except mobile devices), which often contains business-sensitive data.

enisa:physical-attack="theft-of-documents"

Theft of documents

Stealing documents from private/company archives, often for the purpose of re-sale or to achieve personal benefits.

enisa:physical-attack="theft-of-backups"

Theft of backups

Stealing media devices, on which copies of essential information are kept.

enisa:physical-attack="information-leak-or-unauthorised-sharing"

Information leak /sharing

Sharing information with unauthorised entities. Loss of information confidentiality due to intentional human actions (e.g., information leak may occur due to loss of paper copies of confidential information).

enisa:physical-attack="unauthorised-physical-access-or-unauthorised-entry-to-premises"

Unauthorized physical access / Unauthorised entry to premises

Unapproved access to facility.

enisa:physical-attack="coercion-or-extortion-or-corruption"

Coercion, extortion or corruption

Actions following acts of coercion, extortion or corruption.

enisa:physical-attack="damage-from-the-wafare"

Damage from the warfare

Threats of direct impact of warfare activities.

enisa:physical-attack="terrorist-attack"

Terrorist attack

Threats from terrorists.

unintentional-damage

Threats of unintentional human actions or errors.

enisa:unintentional-damage="information-leak-or-sharing-due-to-human-error"

Information leak /sharing due to human error

Information leak / sharing caused by humans, due to their mistakes.

enisa:unintentional-damage="accidental-leaks-or-sharing-of-data-by-employees"

Accidental leaks/sharing of data by employees

Unintentional distribution of private or sensitive data to an unauthorized entity by a staff member.

enisa:unintentional-damage="leaks-of-data-via-mobile-applications"

Leaks of data via mobile applications

Threat of leaking private data (a result of using applications for mobile devices).

enisa:unintentional-damage="leaks-of-data-via-web-applications"

Leaks of data via Web applications

Threat of leaking important information using web applications.

enisa:unintentional-damage="leaks-of-information-transferred-by-network"

Leaks of information transferred by network

Threat of eavesdropping of unsecured network traffic.

enisa:unintentional-damage="erroneous-use-or-administration-of-devices-and-systems"

Erroneous use or administration of devices and systems

Information leak / sharing / damage caused by misuse of IT assets (lack of awareness of application features) or wrong / improper IT assets configuration or management.

enisa:unintentional-damage="loss-of-information-due-to-maintenance-errors-or-operators-errors"

Loss of information due to maintenance errors / operators' errors

Threat of loss of information by incorrectly performed maintenance of devices or systems or other operator activities.

enisa:unintentional-damage="loss-of-information-due-to-configuration-or-installation error"

Loss of information due to configuration/ installation error

Threat of loss of information due to errors in installation or system configuration.

enisa:unintentional-damage="increasing-recovery-time"

Increasing recovery time

Threat of unavailability of information due to errors in the use of backup media and increasing information recovery time.

enisa:unintentional-damage="lost-of-information-due-to-user-errors"

Loss of information due to user errors

Threat of unavailability of information or damage to IT assets caused by user errors (using IT infrastructure) or IT software recovery time.

enisa:unintentional-damage="using-information-from-an-unreliable-source"

Using information from an unreliable source

Bad decisions based on unreliable sources of information or unchecked information.

enisa:unintentional-damage="unintentional-change-of-data-in-an-information-system"

Unintentional change of data in an information system

Loss of information integrity due to human error (information system user mistake).

enisa:unintentional-damage="inadequate-design-and-planning-or-improper-adaptation"

Inadequate design and planning or improper adaptation

Threats caused by improper IT assets or business processes design (inadequate specifications of IT products, inadequate usability, insecure interfaces, policy/procedure flows, design errors).

enisa:unintentional-damage="damage-caused-by-a-third-party"

Damage caused by a third party

Threats of damage to IT assets caused by third party.

enisa:unintentional-damage="security-failure-caused-by-third-party"

Security failure caused by third party

Threats of damage to IT assets caused by breach of security regulations by third party.

enisa:unintentional-damage="damages-resulting-from-penetration-testing"

Damages resulting from penetration testing

Threats to information systems caused by conducting IT penetration tests inappropriately.

enisa:unintentional-damage="loss-of-information-in-the-cloud"

Loss of information in the cloud

Threats of losing information or data stored in the cloud.

enisa:unintentional-damage="loss-of-(integrity-of)-sensitive-information"

Loss of (integrity of) sensitive information

Threats of losing information or data, or changing information classified as sensitive.

enisa:unintentional-damage="loss-of-integrity-of-certificates"

Loss of integrity of certificates

Threat of losing integrity of certificates used for authorisation services

enisa:unintentional-damage="loss-of-devices-and-storage-media-and-documents"

Loss of devices, storage media and documents

Threats of unavailability (losing) of IT assets and documents.

enisa:unintentional-damage="loss-of-devices-or-mobile-devices"

Loss of devices/ mobile devices

Threat of losing mobile devices.

enisa:unintentional-damage="loss-of-storage-media"

Loss of storage media

Threat of losing data-storage media.

enisa:unintentional-damage="loss-of-documentation-of-IT-Infrastructure"

Loss of documentation of IT Infrastructure

Threat of losing important documentation.

enisa:unintentional-damage="destruction-of-records"

Destruction of records

Threats of unavailability (destruction) of data and records (information) stored in devices and storage media.

enisa:unintentional-damage="infection-of-removable-media"

Infection of removable media

Threat of loss of important data due to using removable media, web or mail infection.

enisa:unintentional-damage="abuse-of-storage"

Abuse of storage

Threat of loss of records by improper /unauthorised use of storage devices.

disaster

Threats of damage to information assets caused by natural or environmental factors.

enisa:disaster="disaster"

Disaster (natural earthquakes, floods, landslides, tsunamis, heavy rains, heavy snowfalls, heavy winds)

Large scale natural disasters.

enisa:disaster="fire"

Fire

Threat of fire.

enisa:disaster="pollution-dust-corrosion"

Pollution, dust, corrosion

Threat of disruption of work of IT systems (hardware) due to pollution, dust or corrosion (arising from the air).

enisa:disaster="thunderstrike"

Thunderstrike

Threat of damage to IT hardware caused by thunder strike (overvoltage).

enisa:disaster="water"

Water

Threat of damage to IT hardware caused by water.

enisa:disaster="explosion"

Explosion

Threat of damage to IT hardware caused by explosion.

enisa:disaster="dangerous-radiation-leak"

Dangerous radiation leak

Threat of damage to IT hardware caused by radiation leak.

enisa:disaster="unfavourable-climatic-conditions"

Unfavourable climatic conditions

Threat of disruption of work of IT systems due to climatic conditions that have a negative effect on hardware.

enisa:disaster="loss-of-data-or-accessibility-of-IT-infrastructure-as-a-result-of-heightened-humidity"

Loss of data or accessibility of IT infrastructure as a result of heightened humidity

Threat of disruption of work of IT systems due to high humidity.

enisa:disaster="lost-of-data-or-accessibility-of-IT-infrastructure-as-a-result-of-very-high-temperature"

Lost of data or accessibility of IT infrastructure as a result of very high temperature

Threat of disruption of work of IT systems due to high or low temperature.

enisa:disaster="threats-from-space-or-electromagnetic-storm"

Threats from space / Electromagnetic storm

Threats of the negative impact of solar radiation to satellites and radio wave communication systems - electromagnetic storm.

enisa:disaster="wildlife"

Wildlife

Threat of destruction of IT assets caused by animals: mice, rats, birds.

failures-malfunction

Threat of failure/malfunction of IT supporting infrastructure (i.e. degradation of quality, improper working parameters, jamming). The cause of a failure is mostly an internal issue (e.g.. overload of the power grid in a building).

enisa:failures-malfunction="failure-of-devices-or-systems"

Failure of devices or systems

Threat of failure of IT hardware and/or software assets or its parts.

enisa:failures-malfunction="failure-of-data-media"

Failure of data media

Threat of failure of data media.

enisa:failures-malfunction="hardware-failure"

Hardware failure

Threat of failure of IT hardware.

enisa:failures-malfunction="failure-of-applications-and-services"

Failure of applications and services

Threat of failure of software/applications or services.

enisa:failures-malfunction="failure-of-parts-of-devices-connectors-plug-ins"

Failure of parts of devices (connectors, plug-ins)

Threat of failure of IT equipment or its part.

enisa:failures-malfunction="failure-or-disruption-of-communication-links-communication networks"

Failure or disruption of communication links (communication networks)

Threat of failure or malfunction of communications links.

enisa:failures-malfunction="failure-of-cable-networks"

Failure of cable networks

Threat of failure of communications links due to problems with cable network.

enisa:failures-malfunction="failure-of-wireless-networks"

Failure of wireless networks

Threat of failure of communications links due to problems with wireless networks.

enisa:failures-malfunction="failure-of-mobile-networks"

Failure of mobile networks

Threat of failure of communications links due to problems with mobile networks.

enisa:failures-malfunction="failure-or-disruption-of-main-supply"

Failure or disruption of main supply

Threat of failure or disruption of supply required for information systems.

enisa:failures-malfunction="failure-or-disruption-of-power-supply"

Failure or disruption of power supply

Threat of failure or malfunction of power supply.

enisa:failures-malfunction="failure-of-cooling-infrastructure"

Failure of cooling infrastructure

Threat of failure of IT assets due to improper work of cooling infrastructure.

enisa:failures-malfunction="failure-or-disruption-of-service-providers-supply-chain"

Failure or disruption of service providers (supply chain)

Threat of failure or disruption of third party services required for proper operation of information systems.

enisa:failures-malfunction="malfunction-of-equipment-devices-or-systems"

Malfunction of equipment (devices or systems)

Threat of malfunction of IT hardware and/or software assets or its parts (i.e. improper working parameters, jamming, rebooting).

outages

Threat of complete lack or loss of resources necessary for IT infrastructure. The cause of an outage is mostly an external issue (i.e electricity blackout in the whole city).

enisa:outages="absence-of-personnel"

Absence of personnel

Unavailability of key personnel and their competences.

enisa:outages="strike"

Strike

Unavailability of staff due to a strike (large scale absence of personnel).

enisa:outages="loss-of-support-services"

Loss of support services

Unavailability of support services required for proper operation of the information system.

enisa:outages="internet-outage"

Internet outage

Unavailability of the Internet connection.

enisa:outages="network-outage"

Network outage

Unavailability of communication links.

enisa:outages="outage-of-cable-networks"

Outage of cable networks

Threat of lack of communications links due to problems with cable network.

enisa:outages="Outage-of-short-range-wireless-networks"

Outage of short-range wireless networks

Threat of lack of communications links due to problems with wireless networks (802.11 networks, Bluetooth, NFC etc.).

enisa:outages="outages-of-long-range-wireless-networks"

Outages of long-range wireless networks

Threat of lack of communications links due to problems with mobile networks like cellular network (3G, LTE, GSM etc.) or satellite links.

eavesdropping-interception-hijacking

Threats that alter communication between two parties. These attacks do not have to install additional tools/software on a victim's site.

enisa:eavesdropping-interception-hijacking="war-driving"

War driving

Threat of locating and possibly exploiting connection to the wireless network.

enisa:eavesdropping-interception-hijacking="intercepting-compromising-emissions"

Intercepting compromising emissions

Threat of disclosure of transmitted information using interception and analysis of compromising emission.

enisa:eavesdropping-interception-hijacking="interception-of-information"

Interception of information

Threat of interception of information which is improperly secured in transmission or by improper actions of staff.

enisa:eavesdropping-interception-hijacking="corporate-espionage"

Corporate espionage

Threat of obtaining information secrets by dishonest means.

enisa:eavesdropping-interception-hijacking="nation-state-espionage"

Nation state espionage

Threats of stealing information by nation state espionage (e.g. China based governmental espionage, NSA from USA).

enisa:eavesdropping-interception-hijacking="information-leakage-due-to-unsecured-wi-fi-like-rogue-access-points"

Information leakage due to unsecured Wi-Fi, rogue access points

Threat of obtaining important information by insecure network rogue access points etc.

enisa:eavesdropping-interception-hijacking="interfering-radiation"

Interfering radiation

Threat of failure of IT hardware or transmission connection due to electromagnetic induction or electromagnetic radiation emitted by an outside source.

enisa:eavesdropping-interception-hijacking="replay-of-messages"

Replay of messages

Threat in which valid data transmission is maliciously or fraudulently repeated or delayed.

enisa:eavesdropping-interception-hijacking="network-reconnaissance-network-traffic-manipulation-and-information-gathering"

Network Reconnaissance, Network traffic manipulation and Information gathering

Threat of identifying information about a network to find security weaknesses.

enisa:eavesdropping-interception-hijacking="man-in-the-middle-session-hijacking"

Man in the middle/ Session hijacking

Threats that relay or alter communication between two parties.

legal

Threat of financial or legal penalty or loss of trust of customers and collaborators due to legislation.

enisa:legal="violation-of-rules-and-regulations-breach-of-legislation"

Violation of rules and regulations / Breach of legislation

Threat of financial or legal penalty or loss of trust of customers and collaborators due to violation of law or regulations.

enisa:legal="failure-to-meet-contractual-requirements"

Failure to meet contractual requirements

Threat of financial penalty or loss of trust of customers and collaborators due to failure to meet contractual requirements.

enisa:legal="failure-to-meet-contractual-requirements-by-third-party"

Failure to meet contractual requirements by third party

Threat of financial penalty or loss of trust of customers and collaborators due to a third party's failure to meet contractual requirements

enisa:legal="unauthorized-use-of-IPR-protected-resources"

Unauthorized use of IPR protected resources

Threat of financial or legal penalty or loss of trust of customers and collaborators due to improper/illegal use of IPR protected material (IPR- Intellectual Property Rights.

enisa:legal="illegal-usage-of-file-sharing-services"

Illegal usage of File Sharing services

Threat of financial or legal penalty or loss of trust of customers and collaborators due to improper/illegal use of file sharing services.

enisa:legal="abuse-of-personal-data"

Abuse of personal data

Threat of illegal use of personal data.

enisa:legal="judiciary-decisions-or-court-order"

Judiciary decisions/court order

Threat of financial or legal penalty or loss of trust of customers and collaborators due to judiciary decisions/court order.

nefarious-activity-abuse

Threats of nefarious activities that require use of tools by the attacker. These attacks require installation of additional tools/software or performing additional steps on the victim's IT infrastructure/software.

enisa:nefarious-activity-abuse="identity-theft-identity-fraud-account)"

Identity theft (Identity Fraud/ Account)

Threat of identity theft action.

enisa:nefarious-activity-abuse="credentials-stealing-trojans"

Credentials-stealing trojans

Threat of identity theft action by malware computer programs.

enisa:nefarious-activity-abuse="receiving-unsolicited-e-mail"

Receiving unsolicited E-mail

Threat of receiving unsolicited email which affects information security and efficiency.

enisa:nefarious-activity-abuse="spam"

SPAM

Threat of receiving unsolicited, undesired, or illegal email messages.

enisa:nefarious-activity-abuse="unsolicited-infected-e-mails"

Unsolicited infected e-mails

Threat emanating from unwanted emails that may contain infected attachments or links to malicious / infected web sites.

enisa:nefarious-activity-abuse="denial-of-service"

Denial of service

Threat of service unavailability due to massive requests for services.

enisa:nefarious-activity-abuse="distributed-denial-of-network-service-network-layer-attack"

Distributed denial of network service (DDoS) (network layer attack i.e. Protocol exploitation / Malformed packets / Flooding / Spoofing)

Threat of service unavailability due to a massive number of requests for access to network services from malicious clients.

enisa:nefarious-activity-abuse="distributed-denial-of-network-service-application-layer-attack"

Distributed denial of application service (DDoS) (application layer attack i.e. Ping of Death / XDoS /

WinNuke / HTTP Floods)

Threat of service unavailability due to massive requests sent by multiple malicious clients.

enisa:nefarious-activity-abuse="distributed-denial-of-network-service-amplification-reflection-attack"

Distributed DoS (DDoS) to both network and application services (amplification/reflection methods i.e. NTP/ DNS /…/ BitTorrent)

Threat of creating a massive number of requests, using multiplication/amplification methods.

enisa:nefarious-activity-abuse="malicious-code-software-activity"

Malicious code/ software/ activity

enisa:nefarious-activity-abuse="search-engine-poisoning"

Search Engine Poisoning

Threat of deliberate manipulation of search engine indexes.

enisa:nefarious-activity-abuse="exploitation-of-fake-trust-of-social-media"

Exploitation of fake trust of social media

Threat of malicious activities making use of trusted social media.

enisa:nefarious-activity-abuse="worms-trojans"

Worms/ Trojans

Threat of malware computer programs (trojans/worms).

enisa:nefarious-activity-abuse="rootkits"

Rootkits

Threat of stealthy types of malware software.

enisa:nefarious-activity-abuse="mobile-malware"

Mobile malware

Threat of mobile malware programs.

enisa:nefarious-activity-abuse="infected-trusted-mobile-apps"

Infected trusted mobile apps

Threat of using mobile malware software that is recognised as trusted one.

enisa:nefarious-activity-abuse="elevation-of-privileges"

Elevation of privileges

Threat of exploiting bugs, design flaws or configuration oversights in an operating system or software application to gain elevated access to resources.

enisa:nefarious-activity-abuse="web-application-attacks-injection-attacks-code-injection-SQL-XSS"

Web application attacks / injection attacks (Code injection: SQL, XSS)

Threat of utilizing custom web applications embedded within social media sites, which can lead to installation of malicious code onto computers to be used to gain unauthorized access.

enisa:nefarious-activity-abuse="spyware-or-deceptive-adware"

Spyware or deceptive adware

Threat of using software that aims to gather information about a person or organization without their knowledge.

enisa:nefarious-activity-abuse="viruses"

Viruses

Threat of infection by viruses.

enisa:nefarious-activity-abuse="rogue-security-software-rogueware-scareware"

Rogue security software/ Rogueware / Scareware

Threat of internet fraud or malicious software that mislead users into believing there is a virus on their computer, and manipulates them to pay money for fake removal tool.

enisa:nefarious-activity-abuse="ransomware"

Ransomware

Threat of infection of computer system or device by malware that restricts access to it and demands that the user pay a ransom to remove the restriction.

enisa:nefarious-activity-abuse="exploits-exploit-kits"

Exploits/Exploit Kits

Threat to IT assets due to the use of web available exploits or exploits software.

enisa:nefarious-activity-abuse="social-engineering"

Social Engineering

Threat of social engineering type attacks (target: manipulation of personnel behaviour).

enisa:nefarious-activity-abuse="phishing-attacks"

Phishing attacks

Threat of an email fraud method in which the perpetrator sends out legitimate-looking email in an attempt to gather personal and financial information from recipients. Typically, the messages appear to come from well-known and trustworthy websites.

enisa:nefarious-activity-abuse="spear-phishing-attacks"

Spear phishing attacks

Spear-phishing is a targeted e-mail message that has been crafted to create fake trust and thus lure the victim to unveil some business or personal secrets that can be abused by the adversary.

enisa:nefarious-activity-abuse="abuse-of-information-leakage"

Abuse of Information Leakage

Threat of leaking important information.

enisa:nefarious-activity-abuse="leakage-affecting-mobile-privacy-and-mobile-applications"

Leakage affecting mobile privacy and mobile applications

Threat of leaking important information due to using malware mobile applications.

enisa:nefarious-activity-abuse="leakage-affecting-web-privacy-and-web-applications"

Leakage affecting web privacy and web applications

Threat of leakage important information due to using malware web applications.

enisa:nefarious-activity-abuse="leakage-affecting-network-traffic"

Leakage affecting network traffic

Threat of leaking important information in network traffic.

enisa:nefarious-activity-abuse="leakage-affecting-cloud-computing"

Leakage affecting cloud computing

Threat of leaking important information in cloud computing.

enisa:nefarious-activity-abuse="generation-and-use-of-rogue-certificates"

Generation and use of rogue certificates

Threat of use of rogue certificates.

enisa:nefarious-activity-abuse="loss-of-integrity-of-sensitive-information"

Loss of (integrity of) sensitive information

Threat of loss of sensitive information due to loss of integrity.

enisa:nefarious-activity-abuse="man-in-the-middle-session-hijacking"

Man in the middle / Session hijacking

Threat of attack consisting in the exploitation of the web session control mechanism, which is normally managed by a session token.

enisa:nefarious-activity-abuse="social-engineering-via-signed-malware"

Social Engineering / signed malware

Threat of install fake trust signed software (malware) e.g. fake OS updates.

enisa:nefarious-activity-abuse="fake-SSL-certificates"

Fake SSL certificates

Threat of attack due to malware application signed by a certificate that is typically inherently trusted by an endpoint.

enisa:nefarious-activity-abuse="manipulation-of-hardware-and-software"

Manipulation of hardware and software

Threat of unauthorised manipulation of hardware and software.

enisa:nefarious-activity-abuse="anonymous-proxies"

Anonymous proxies

Threat of unauthorised manipulation by anonymous proxies.

enisa:nefarious-activity-abuse="abuse-of-computing-power-of-cloud-to-launch-attacks-cybercrime-as-a-service)"

Abuse of computing power of cloud to launch attacks (cybercrime as a service)

Threat of using large computing powers to generate attacks on demand.

enisa:nefarious-activity-abuse="abuse-of-vulnerabilities-0-day-vulnerabilities"

Abuse of vulnerabilities, 0-day vulnerabilities

Threat of attacks using 0-day or known IT assets vulnerabilities.

enisa:nefarious-activity-abuse="access-of-web-sites-through-chains-of-HTTP-Proxies-Obfuscation"

Access of web sites through chains of HTTP Proxies (Obfuscation)

Threat of bypassing the security mechanism using HTTP proxies (bypassing the website blacklist).

enisa:nefarious-activity-abuse="access-to-device-software"

Access to device software

Threat of unauthorised manipulation by access to device software.

enisa:nefarious-activity-abuse="alternation-of-software"

Alternation of software

Threat of unauthorized modifications to code or data, attacking its integrity.

enisa:nefarious-activity-abuse="rogue-hardware"

Rogue hardware

Threat of manipulation due to unauthorized access to hardware.

enisa:nefarious-activity-abuse="manipulation-of-information"

Manipulation of information

Threat of intentional data manipulation to mislead information systems or somebody or to cover other nefarious activities (loss of integrity of information).

enisa:nefarious-activity-abuse="repudiation-of-actions"

Repudiation of actions

Threat of intentional data manipulation to repudiate action.

enisa:nefarious-activity-abuse="address-space-hijacking-IP-prefixes"

Address space hijacking (IP prefixes)

Threat of the illegitimate takeover of groups of IP addresses.

enisa:nefarious-activity-abuse="routing-table-manipulation"

Routing table manipulation

Threat of route packets of network to IP addresses other than that was intended via sender by unauthorised manipulation of routing table.

enisa:nefarious-activity-abuse="DNS-poisoning-or-DNS-spoofing-or-DNS-Manipulations"

DNS poisoning / DNS spoofing / DNS Manipulations

Threat of falsification of DNS information.

enisa:nefarious-activity-abuse="falsification-of-record"

Falsification of record

Threat of intentional data manipulation to falsify records.

enisa:nefarious-activity-abuse="autonomous-system-hijacking"

Autonomous System hijacking

Threat of overtaking by the attacker the ownership of a whole autonomous system and its prefixes despite origin validation.

enisa:nefarious-activity-abuse="autonomous-system-manipulation"

Autonomous System manipulation

Threat of manipulation by the attacker of a whole autonomous system in order to perform malicious actions.

enisa:nefarious-activity-abuse="falsification-of-configurations"

Falsification of configurations

Threat of intentional manipulation due to falsification of configurations.

enisa:nefarious-activity-abuse="misuse-of-audit-tools"

Misuse of audit tools

Threat of nefarious actions performed using audit tools (discovery of security weaknesses in information systems)

enisa:nefarious-activity-abuse="misuse-of-information-or-information systems-including-mobile-apps"

Misuse of information/ information systems (including mobile apps)

Threat of nefarious action due to misuse of information / information systems.

enisa:nefarious-activity-abuse="unauthorized-activities"

Unauthorized activities

Threat of nefarious action due to unauthorised activities.

enisa:nefarious-activity-abuse="Unauthorised-use-or-administration-of-devices-and-systems"

Unauthorised use or administration of devices and systems

Threat of nefarious action due to unauthorised use of devices and systems.

enisa:nefarious-activity-abuse="unauthorised-use-of-software"

Unauthorised use of software

Threat of nefarious action due to unauthorised use of software.

enisa:nefarious-activity-abuse="unauthorized-access-to-the-information-systems-or-networks-like-IMPI-Protocol-DNS-Registrar-Hijacking)"

Unauthorized access to the information systems-or-networks (IMPI Protocol / DNS Registrar Hijacking)

Threat of unauthorised access to the information systems / network.

enisa:nefarious-activity-abuse="network-intrusion"

Network Intrusion

Threat of unauthorised access to network.

enisa:nefarious-activity-abuse="unauthorized-changes-of-records"

Unauthorized changes of records

Threat of unauthorised changes of information.

enisa:nefarious-activity-abuse="unauthorized-installation-of-software"

Unauthorized installation of software

Threat of unauthorised installation of software.

enisa:nefarious-activity-abuse="Web-based-attacks-drive-by-download-or-malicious-URLs-or-browser-based-attacks"

Web based attacks (Drive-by download / malicious URLs / Browser based attacks)

Threat of installation of unwanted malware software by misusing websites.

enisa:nefarious-activity-abuse="compromising-confidential-information-like-data-breaches"

Compromising confidential information (data breaches)

Threat of data breach.

enisa:nefarious-activity-abuse="hoax"

Hoax

Threat of loss of IT assets security due to cheating.

enisa:nefarious-activity-abuse="false-rumour-and-or-fake-warning"

False rumour and/or fake warning

Threat of disruption of work due to rumours and/or a fake warning.

enisa:nefarious-activity-abuse="remote-activity-execution"

Remote activity (execution)

Threat of nefarious action by attacker remote activity.

enisa:nefarious-activity-abuse="remote-command-execution"

Remote Command Execution

Threat of nefarious action due to remote command execution.

enisa:nefarious-activity-abuse="remote-access-tool"

Remote Access Tool (RAT)

Threat of infection of software that has a remote administration capabilities allowing an attacker to control the victim’s computer.

enisa:nefarious-activity-abuse="botnets-remote-activity"

Botnets / Remote activity

Threat of penetration by software from malware distribution.

enisa:nefarious-activity-abuse="targeted-attacks"

Targeted attacks (APTs etc.)

Threat of sophisticated, targeted attack which combine many attack techniques.

enisa:nefarious-activity-abuse="mobile-malware-exfiltration"

Mobile malware (exfiltration)

Threat of mobile software that aims to gather information about a person or organization without their knowledge.

enisa:nefarious-activity-abuse="spear-phishing-attacks-targeted"

Spear phishing attacks (targeted)

Threat of attack focused on a single user or department within an organization, coming from someone within the company in a position of trust and requesting information such as login, IDs and passwords.

enisa:nefarious-activity-abuse="installation-of-sophisticated-and-targeted-malware"

Installation of sophisticated and targeted malware

Threat of malware delivered by sophisticated and targeted software.

enisa:nefarious-activity-abuse="watering-hole-attacks"

Watering Hole attacks

Threat of malware residing on the websites which a group often uses.

enisa:nefarious-activity-abuse="failed-business-process"

Failed business process

Threat of damage or loss of IT assets due to improperly executed business process.

enisa:nefarious-activity-abuse="brute-force"

Brute force

Threat of unauthorised access via systematically checking all possible keys or passwords until the correct one is found.

enisa:nefarious-activity-abuse="abuse-of-authorizations"

Abuse of authorizations

Threat of using authorised access to perform illegitimate actions.

estimative-language

estimative-language namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Estimative language to describe quality and credibility of underlying sources, data, and methodologies based Intelligence Community Directive 203 (ICD 203)

likelihood-probability

Properly expresses and explains uncertainties associated with major analytic judgments: Analytic products should indicate and explain the basis for the uncertainties associated with major analytic judgments, specifically the likelihood of occurrence of an event or development, and the analyst's confidence in the basis for this judgment. Degrees of likelihood encompass a full spectrum from remote to nearly certain. Analysts' confidence in an assessment or judgment may be based on the logic and evidentiary base that underpin it, including the quantity and quality of source material, and their understanding of the topic. Analytic products should note causes of uncertainty (e.g., type, currency, and amount of information, knowledge gaps, and the nature of the issue) and explain how uncertainties affect analysis (e.g., to what degree and how a judgment depends on assumptions). As appropriate, products should identify indicators that would alter the levels of uncertainty for major analytic judgments. Consistency in the terms used and the supporting information and logic advanced is critical to success in expressing uncertainty, regardless of whether likelihood or confidence expressions are used.

estimative-language:likelihood-probability="almost-no-chance"

Almost no chance - remote - 01-05%

estimative-language:likelihood-probability="very-unlikely"

Very unlikely - highly improbable - 05-20%

Associated numerical value="5"

estimative-language:likelihood-probability="unlikely"

Unlikely - improbable (improbably) - 20-45%

Associated numerical value="20"

estimative-language:likelihood-probability="roughly-even-chance"

Roughly even change - roughly even odds - 45-55%

Associated numerical value="45"

estimative-language:likelihood-probability="likely"

Likely - probable (probably) - 55-80%

Associated numerical value="55"

estimative-language:likelihood-probability="very-likely"

Very likely - highly probable - 80-95%

Associated numerical value="80"

estimative-language:likelihood-probability="almost-certain"

Almost certain(ly) - nearly certain - 95-99%

Associated numerical value="95"

eu-marketop-and-publicadmin

eu-marketop-and-publicadmin namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Market operators and public administrations that must comply to some notifications requirements under EU NIS directive

critical-infra-operators

eu-marketop-and-publicadmin:critical-infra-operators="transport"

Transport

eu-marketop-and-publicadmin:critical-infra-operators="energy"

Energy

eu-marketop-and-publicadmin:critical-infra-operators="health"

Health

eu-marketop-and-publicadmin:critical-infra-operators="financial"

Financial market operators

eu-marketop-and-publicadmin:critical-infra-operators="banking"

Banking

info-services

eu-marketop-and-publicadmin:info-services="e-commerce"

e-commerce platforms

eu-marketop-and-publicadmin:info-services="internet-payment"

Internet payment

eu-marketop-and-publicadmin:info-services="cloud"

cloud computing

eu-marketop-and-publicadmin:info-services="search-engines"

search engines

eu-marketop-and-publicadmin:info-services="socnet"

social networks

eu-marketop-and-publicadmin:info-services="app-stores"

application stores

public-admin

eu-marketop-and-publicadmin:public-admin="public-admin"

Public Administrations

euci

euci namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

EU classified information (EUCI) means any information or material designated by a EU security classification, the unauthorised disclosure of which could cause varying degrees of prejudice to the

interests of the European Union or of one or more of the Member States.

TS-UE/EU-TS

Information and material the unauthorised disclosure of which could cause exceptionally grave prejudice to the essential interests of the European Union or of one or more of the Member States.

euci:TS-UE/EU-TS

TRES SECRET UE/EU TOP SECRET

Information and material the unauthorised disclosure of which could cause exceptionally grave prejudice to the essential interests of the European Union or of one or more of the Member States.

S-UE/EU-S

Information and material the unauthorised disclosure of which could seriously harm the essential interests of the European Union or of one or more of the Member States.

euci:S-UE/EU-S

SECRET UE/EU SECRET

Information and material the unauthorised disclosure of which could seriously harm the essential interests of the European Union or of one or more of the Member States.

C-UE/EU-C

Information and material the unauthorised disclosure of which could harm the essential interests of the European Union or of one or more of the Member States.

euci:C-UE/EU-C

CONFIDENTIEL UE/EU CONFIDENTIAL

Information and material the unauthorised disclosure of which could harm the essential interests of the European Union or of one or more of the Member States.

R-UE/EU-R

Information and material the unauthorised disclosure of which could be disadvantageous to the interests of the European Union or of one or more of the Member States.

euci:R-UE/EU-R

RESTREINT UE/EU RESTRICTED

Information and material the unauthorised disclosure of which could be disadvantageous to the

interests of the European Union or of one or more of the Member States.

europol-event

europol-event namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

This taxonomy was designed to describe the type of events

infected-by-known-malware

The presence of any of the types of malware was detected in a system.

europol-event:infected-by-known-malware

System(s) infected by known malware

The presence of any of the types of malware was detected in a system.

dissemination-malware-email

Malware attached to a message or email message containing link to malicious URL.

europol-event:dissemination-malware-email

Dissemination of malware by email

Malware attached to a message or email message containing link to malicious URL.

hosting-malware-webpage

```
Web page disseminating one or various types of malware.
```

europol-event:hosting-malware-webpage

Hosting of malware on web page

```
Web page disseminating one or various types of malware.
```

c&c-server-hosting

Web page disseminating one or various types of malware.

europol-event:c&c-server-hosting

Hosting of malware on web page

Web page disseminating one or various types of malware.

worm-spreading

System infected by a worm trying to infect other systems.

europol-event:worm-spreading

Replication and spreading of a worm

System infected by a worm trying to infect other systems.

connection-malware-port

System attempting to gain access to a port normally linked to a specific type of malware.

europol-event:connection-malware-port

Connection to (a) suspicious port(s) linked to specific malware

System attempting to gain access to a port normally linked to a specific type of malware.

connection-malware-system

System attempting to gain access to an IP address or URL normally linked to a specific type of malware, e.g. C&C or a distribution page for components linked to a specific botnet.

europol-event:connection-malware-system

Connection to (a) suspicious system(s) linked to specific malware

System attempting to gain access to an IP address or URL normally linked to a specific type of malware, e.g. C&C or a distribution page for components linked to a specific botnet.

flood

Mass mailing of requests (network packets, emails, etc…) from one single source to a specific service, aimed at affecting its normal functioning.

europol-event:flood

Flood of requests

Mass mailing of requests (network packets, emails, etc…) from one single source to a specific

service, aimed at affecting its normal functioning.

exploit-tool-exhausting-resources

One single source using specially designed software to affect the normal functioning of a specific service, by exploiting a vulnerability.

europol-event:exploit-tool-exhausting-resources

Exploit or tool aimed at exhausting resources (network, processing capacity, sessions, etc…)

One single source using specially designed software to affect the normal functioning of a specific service, by exploiting a vulnerability.

packet-flood

Mass mailing of requests (network packets, emails, etc…) from various sources to a specific service, aimed at affecting its normal functioning.

europol-event:packet-flood

Packet flooding

Mass mailing of requests (network packets, emails, etc…) from various sources to a specific service, aimed at affecting its normal functioning.

exploit-framework-exhausting-resources

Various sources using specially designed software to affect the normal functioning of a specific service, by exploiting a vulnerability.

europol-event:exploit-framework-exhausting-resources

Exploit or tool distribution aimed at exhausting resources

Various sources using specially designed software to affect the normal functioning of a specific service, by exploiting a vulnerability.

vandalism

Logical and physical activities which – although they are not aimed at causing damage to information or at preventing its transmission among systems – have this effect.

europol-event:vandalism

Vandalism

Logical and physical activities which – although they are not aimed at causing damage to

information or at preventing its transmission among systems – have this effect.

disruption-data-transmission

Logical and physical activities aimed at causing damage to information or at preventing its transmission among systems.

europol-event:disruption-data-transmission

Intentional disruption of data transmission and processing mechanisms

Logical and physical activities aimed at causing damage to information or at preventing its transmission among systems.

system-probe

Single system scan searching for open ports or services using these ports for responding.

europol-event:system-probe

System probe

Single system scan searching for open ports or services using these ports for responding.

network-scanning

Scanning a network aimed at identifying systems which are active in the same network.

europol-event:network-scanning

Network scanning

Scanning a network aimed at identifying systems which are active in the same network.

dns-zone-transfer

Transfer of a specific DNS zone.

europol-event:dns-zone-transfer

DNS zone transfer

Transfer of a specific DNS zone.

wiretapping

Logical or physical interception of communications.

europol-event:wiretapping

Wiretapping

Logical or physical interception of communications.

dissemination-phishing-emails

Mass emailing aimed at collecting data for phishing purposes with regard to the victims.

europol-event:dissemination-phishing-emails

Dissemination of phishing emails

Mass emailing aimed at collecting data for phishing purposes with regard to the victims.

hosting-phishing-sites

Hosting web sites for phishing purposes.

europol-event:hosting-phishing-sites

Hosting phishing sites

Hosting web sites for phishing purposes.

aggregation-information-phishing-schemes

Collecting data obtained through phishing attacks on web pages, email accounts, etc…

europol-event:aggregation-information-phishing-schemes

Aggregation of information gathered through phishing schemes

Collecting data obtained through phishing attacks on web pages, email accounts, etc…

exploit-attempt

Unsuccessful use of a tool exploiting a specific vulnerability of the system.

europol-event:exploit-attempt

Exploit attempt

Unsuccessful use of a tool exploiting a specific vulnerability of the system.

sql-injection-attempt

Unsuccessful attempt to manipulate or read the information of a database by using the SQL injection technique.

europol-event:sql-injection-attempt

SQL injection attempt

Unsuccessful attempt to manipulate or read the information of a database by using the SQL injection technique.

xss-attempt

Unsuccessful attempts to perform attacks by using cross-site scripting techniques.

europol-event:xss-attempt

XSS attempt

Unsuccessful attempts to perform attacks by using cross-site scripting techniques.

file-inclusion-attempt

Unsuccessful attempt to include files in the system under attack by using file inclusion techniques.

europol-event:file-inclusion-attempt

File inclusion attempt

Unsuccessful attempt to include files in the system under attack by using file inclusion techniques.

brute-force-attempt

Unsuccessful login attempt by using sequential credentials for gaining access to the system.

europol-event:brute-force-attempt

Brute force attempt

Unsuccessful login attempt by using sequential credentials for gaining access to the system.

password-cracking-attempt

Attempt to acquire access credentials by breaking the protective cryptographic keys.

europol-event:password-cracking-attempt

Password cracking attempt

Attempt to acquire access credentials by breaking the protective cryptographic keys.

dictionary-attack-attempt

Unsuccessful login attempt by using system access credentials previously loaded into a dictionary.

europol-event:dictionary-attack-attempt

Dictionary attack attempt

Unsuccessful login attempt by using system access credentials previously loaded into a dictionary.

exploit

Successful use of a tool exploiting a specific vulnerability of the system.

europol-event:exploit

Use of a local or remote exploit

Successful use of a tool exploiting a specific vulnerability of the system.

sql-injection

Manipulation or reading of information contained in a database by using the SQL injection technique.

europol-event:sql-injection

SQL injection

Manipulation or reading of information contained in a database by using the SQL injection technique.

xss

Attacks performed with the use of cross-site scripting techniques.

europol-event:xss

XSS

Attacks performed with the use of cross-site scripting techniques.

file-inclusion

Inclusion of files into a system under attack with the use of file inclusion techniques.

europol-event:file-inclusion

File inclusion

Inclusion of files into a system under attack with the use of file inclusion techniques.

control-system-bypass

Unauthorised access to a system or component by bypassing an access control system in place.

europol-event:control-system-bypass

Control system bypass

Unauthorised access to a system or component by bypassing an access control system in place.

theft-access-credentials

Unauthorised access to a system or component by using stolen access credentials.

europol-event:theft-access-credentials

Theft of access credentials

Unauthorised access to a system or component by using stolen access credentials.

unauthorized-access-system

Unauthorised access to a system or component.

europol-event:unauthorized-access-system

Unauthorised access to a system

Unauthorised access to a system or component.

unauthorized-access-information

Unauthorised access to a set of information.

europol-event:unauthorized-access-information

Unauthorised access to information

Unauthorised access to a set of information.

data-exfiltration

Unauthorised access to and sharing of a specific set of information.

europol-event:data-exfiltration

Data exfiltration

Unauthorised access to and sharing of a specific set of information.

modification-information

Unauthorised changes to a specific set of information.

europol-event:modification-information

Modification of information

Unauthorised changes to a specific set of information.

deletion-information

Unauthorised deleting of a specific set of information.

europol-event:deletion-information

Deletion of information

Unauthorised deleting of a specific set of information.

illegitimate-use-resources

Use of institutional resources for purposes other than those intended.

europol-event:illegitimate-use-resources

Misuse or unauthorised use of resources

Use of institutional resources for purposes other than those intended.

illegitimate-use-name

Using the name of an institution without permission to do so.

europol-event:illegitimate-use-name

Illegitimate use of the name of an institution or third party

Using the name of an institution without permission to do so.

email-flooding

Sending an unusually large quantity of email messages.

europol-event:email-flooding

Email flooding

Sending an unusually large quantity of email messages.

spam

Sending an email message that was unsolicited or unwanted by the recipient.

europol-event:spam

Sending an unsolicited message

Sending an email message that was unsolicited or unwanted by the recipient.

copyrighted-content

Distribution or sharing of content protected by copyright and related rights.

europol-event:copyrighted-content

Distribution or sharing of copyright protected content

Distribution or sharing of content protected by copyright and related rights.

content-forbidden-by-law

Distribution or sharing of illegal content such as child pornography, racism, xenophobia, etc…

europol-event:content-forbidden-by-law

Dissemination of content forbidden by law (publicly prosecuted offences)

Distribution or sharing of illegal content such as child pornography, racism, xenophobia, etc…

unspecified

Other unlisted events.

europol-event:unspecified

Other unspecified event

Other unlisted events.

undetermined

Field aimed at the classification of unprocessed events, which have remained undetermined from the beginning.

europol-event:undetermined

Undetermined

Field aimed at the classification of unprocessed events, which have remained undetermined from the beginning.

europol-incident

europol-incident namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

This taxonomy was designed to describe the type of incidents by class.

malware

europol-incident:malware="infection"

Infection

Infecting one or various systems with a specific type of malware.

europol-incident:malware="distribution"

Distribution

Infecting one or various systems with a specific type of malware.

europol-incident:malware="c&c"

C&C

Infecting one or various systems with a specific type of malware.

europol-incident:malware="undetermined"

Undetermined

availability

europol-incident:availability="dos-ddos"

DoS/DDoS

Disruption of the processing and response capacity of systems and networks in order to render them inoperative.

europol-incident:availability="sabotage"

Sabotage

Premeditated action to damage a system, interrupt a process, change or delete information, etc.

information-gathering

europol-incident:information-gathering="scanning"

Scanning

Active and passive gathering of information on systems or networks.

europol-incident:information-gathering="sniffing"

Sniffing

Unauthorised monitoring and reading of network traffic.

europol-incident:information-gathering="phishing"

Phishing

Attempt to gather information on a user or a system through phishing methods.

intrusion-attempt

europol-incident:intrusion-attempt="exploitation-vulnerability"

Exploitation of vulnerability

Attempt to intrude by exploiting a vulnerability in a system, component or network.

europol-incident:intrusion-attempt="login-attempt"

Login attempt

Attempt to log in to services or authentication / access control mechanisms.

intrusion

europol-incident:intrusion="exploitation-vulnerability"

Exploitation of vulnerability

Actual intrusion by exploiting a vulnerability in the system, component or network.

europol-incident:intrusion="compromising-account"

Compromising an account

Actual intrusion in a system, component or network by compromising a user or administrator account.

information-security

europol-incident:information-security="unauthorized-access"

Unauthorised access

Unauthorised access to a particular set of information

europol-incident:information-security="unauthorized-modification"

Unauthorised modification/deletion

Unauthorised change or elimination of a particular set of information

fraud

europol-incident:fraud="illegitimate-use-resources"

Misuse or unauthorised use of resources

Use of institutional resources for purposes other than those intended.

europol-incident:fraud="illegitimate-use-name"

Illegitimate use of the name of a third party

Use of the name of an institution without permission to do so.

abusive-content

europol-incident:abusive-content="spam"

SPAM

```
Sending SPAM messages.
```

europol-incident:abusive-content="copyright"

Copyright

Distribution and sharing of copyright protected content.

europol-incident:abusive-content="content-forbidden-by-law"

Dissemination of content forbidden by law.

Child pornography, racism and apology of violence.

other

europol-incident:other="other"

Other

```
Other type of unspecified incident
```

event-assessment

event-assessment namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

A series of assessment predicates describing the event assessment performed to make judgement(s) under a certain level of uncertainty.

alternative-points-of-view-process

A list of procedures or practices which describe alternative points of view to validate or rate an analysis. The list describes techniques or methods which could reinforce the estimative language in a human analysis and/or challenge the assumptions to reduce the potential bias of the analysis introduced by the analyst(s).

event-assessment:alternative-points-of-view-process="analytic-debates-within-the-organisation"

analytic debates within the organisation

event-assessment:alternative-points-of-view-process="devils-advocates-methodology"

Devil’s advocates methodlogy

event-assessment:alternative-points-of-view-process="competitive-analysis"

competitive analysis

event-assessment:alternative-points-of-view-process="interdisciplinary-brainstorming"

interdisciplinary brainstorming

event-assessment:alternative-points-of-view-process="intra-office-peer-review"

intra-office peer review

event-assessment:alternative-points-of-view-process="outside-expertise-review"

Outside expertise review

fr-classif

fr-classif namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

French gov information classification system

Exclusive flag set which means the values or predicate below must be set exclusively.

classifiees-defense

Exclusive flag set which means the values or predicate below must be set exclusively.

fr-classif:classifiees-defense="TRES_SECRET_DEFENSE"

TRES SECRET DEFENSE

fr-classif:classifiees-defense="SECRET_DEFENSE"

SECRET DEFENSE

fr-classif:classifiees-defense="CONFIDENTIEL_DEFENSE"

CONFIDENTIEL DEFENSE

non-classifiees-defense

Exclusive flag set which means the values or predicate below must be set exclusively.

fr-classif:non-classifiees-defense="SECRET"

SECRET

fr-classif:non-classifiees-defense="CONFIDENTIEL"

CONFIDENTIEL

fr-classif:non-classifiees-defense="DIFFUSION_RESTREINTE"

DIFFUSION RESTREINTE

non-classifiees

Exclusive flag set which means the values or predicate below must be set exclusively.

fr-classif:non-classifiees="NON-CLASSIFIEES"

NON CLASSIFIEES

honeypot-basic

honeypot-basic namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Christian Seifert, Ian Welch, Peter Komisarczuk, 'Taxonomy of Honeypots', Technical Report CS-TR-06/12, VICTORIA UNIVERSITY OF WELLINGTON, School of Mathematical and Computing Sciences,

June 2006, http://www.mcs.vuw.ac.nz/comp/Publications/archive/CS-TR-06/CS-TR-06-12.pdf

interaction-level

Describes whether the exposed functionality of a honeypot is limited in some way, which is usually the case for honeypots that simulate services.

honeypot-basic:interaction-level="high"

High Interaction Level

Exposed functionality of the honeypot is not limited.

honeypot-basic:interaction-level="low"

low Interaction Level

Exposed functionality being limited. For example, a simulated SSH server of a honeypot is not able to authenticate against a valid login/password combination

data-capture

Describes the type of data a honeypot is able to capture

honeypot-basic:data-capture="events"

Events

The honeypot collects data about something that has happened or took place, a change in state.

honeypot-basic:data-capture="attacks"

Attacks

The honeypot collects malicious activity.

honeypot-basic:data-capture="intrusions"

Intrusions

The honeypot collects malicious activity that leads to a security failure.

honeypot-basic:data-capture="none"

None

The honeypot does not collect events, attacks, or intrusions.

containment

Classifies the measures a honeypot takes to defend against malicious activity spreading from itself.

honeypot-basic:containment="block"

Block

Attacker’s actions are identified and blocked. The attack never reaches the target.

honeypot-basic:containment="defuse"

Defuse

The attack reaches the target, but is manipulated in a way that it fails against the target.

honeypot-basic:containment="slow-down"

Slow Down

Attacker is slowed down in his actions of spreading malicious activity.

honeypot-basic:containment="none"

None

No action is taken to limit the intruder’s spread of malicious activity against other systems.

distribution-appearance

Describes whether the honeypot system appears to be confined to one system or multiple systems.

honeypot-basic:distribution-appearance="distributed"

Distributed

The honeypot is or appears to be composed of multiple systems.

honeypot-basic:distribution-appearance="stand-alone"

Stand-Alone

The honeypot is or appears to be one system.

communication-interface

Describes the interfaces one can use to interact directly with the honeypot.

honeypot-basic:communication-interface="network-interface"

Network Interface

The honeypot can be directly communicated with via a network interface.

honeypot-basic:communication-interface="hardware-interface"

Non-Network Hardware Interface

Examples: Printer port, CDROM drives, USB connections.

honeypot-basic:communication-interface="software-api"

Software API

The honeypot can be interacted with via a software API.

role

Describes in what role the honeypot acts within a multi-tier architecture.

honeypot-basic:role="server"

Server

The honeypot is passively awaiting requests from clients.

honeypot-basic:role="client"

Client

The honeypot is actively initiating requests to servers.

iep

iep namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Forum of Incident Response and Security Teams (FIRST) Information Exchange Policy (IEP) framework

commercial-use

States whether Recipients are permitted to use information received in commercial products or services.

iep:commercial-use="MAY"

Recipients MAY use this information in commercial products or services.

iep:commercial-use="MUST NOT"

Recipients MUST NOT use this information in commercial products or services.

external-reference

This statement can be used to convey a description or reference to any applicable licenses, agreements, or conditions between the producer and receiver.

iep:external-reference="$text"

An external-reference value is required

encrypt-in-transit

States whether the received information has to be encrypted when it is retransmitted by the recipient.

iep:encrypt-in-transit="MUST"

Recipients MUST encrypt the information received when it is retransmitted or redistributed.

iep:encrypt-in-transit="MAY"

Recipients MAY encrypt the information received when it is retransmitted or redistributed.

encrypt-at-rest

States whether the received information has to be encrypted by the Recipient when it is stored at rest.

iep:encrypt-at-rest="MUST"

Recipients MUST encrypt the information received when it is stored at rest.

iep:encrypt-at-rest="MAY"

Recipients MAY encrypt the information received when it is stored at rest.

permitted-actions

States the permitted actions that Recipients can take upon information received.

iep:permitted-actions="NONE"

Recipients MUST contact the Providers before acting upon the information received.

iep:permitted-actions="CONTACT FOR INSTRUCTION"

Recipients MUST contact the Providers before acting upon the information received.

iep:permitted-actions="INTERNALLY VISIBLE ACTIONS"

Recipients MAY conduct actions on the information received that are only visible on the Recipients internal networks and systems, and MUST NOT conduct actions that are visible outside of the Recipients networks and systems, or visible to third parties.

iep:permitted-actions="EXTERNALLY VISIBLE INDIRECT ACTIONS"

Recipients MAY conduct indirect, or passive, actions on the information received that are externally visible and MUST NOT conduct direct, or active, actions.

iep:permitted-actions="EXTERNALLY VISIBLE DIRECT ACTIONS"

Recipients MAY conduct direct, or active, actions on the information received that are externally visible.

affected-party-notifications

Recipients are permitted notify affected third parties of a potential compromise or threat.

iep:affected-party-notifications="MAY"

Recipients MAY notify affected parties of a potential compromise or threat.

iep:affected-party-notifications="MUST NOT"

Recipients MUST NOT notify affected parties of potential compromise or threat.

traffic-light-protocol

Recipients are permitted to redistribute the information received within the redistribution scope as defined by the enumerations.

iep:traffic-light-protocol="RED"

Personal for identified recipients only.

iep:traffic-light-protocol="AMBER"

Limited sharing on the basis of need-to-know.

iep:traffic-light-protocol="GREEN"

Community wide sharing.

iep:traffic-light-protocol="WHITE"

Unlimited sharing.

provider-attribution

Recipients could be required to attribute or anonymize the Provider when redistributing the information received.

iep:provider-attribution="MAY"

Recipients MAY attribute the Provider when redistributing the information received.

iep:provider-attribution="MUST"

Recipients MUST attribute the Provider when redistributing the information received.

iep:provider-attribution="MUST NOT"

Recipients MUST NOT attribute the Provider when redistributing the information received.

obfuscate-affected-parties

Recipients could be required to obfuscate or anonymize information that could be used to identify the victims before redistributing the information received.

iep:obfuscate-affected-parties="MAY"

Recipients MAY obfuscate information about the specific affected parties.

iep:obfuscate-affected-parties="MUST"

Recipients MUST obfuscate information about the specific affected parties.

iep:obfuscate-affected-parties="MUST NOT"

Recipients MUST NOT obfuscate information about the specific affected parties.

unmodified-resale

States whether the recipient MAY or MUST NOT resell the information received unmodified or in a semantically equivalent format.

iep:unmodified-resale="MAY"

Recipients MAY resell the information received.

iep:unmodified-resale="MUST NOT"

Recipients MUST NOT resell the information received unmodified or in a semantically equivalent format.

start-date

States the UTC date that the IEP is effective from.

iep:start-date="$text"

A start-date value is required

end-date

States the UTC date that the IEP is effective until.

iep:end-date="$text"

An end-date value is required

reference

This statement can be used to provide a URL reference to the specific IEP implementation.

iep:reference="$text"

A reference value is required

name

This statement can be used to provide a name for an IEP implementation.

iep:name="$text"

A name value is required

version

States the version of the IEP framework that has been used.

iep:version="$text"

A version value is required

id

Provides a unique ID to identify a specific IEP implementation.

iep:id="$text"

An id value is required

incident-disposition

incident-disposition namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

How an incident is classified in its process to be resolved. The taxonomy is inspired from NASA Incident Response and Management Handbook. https://www.nasa.gov/pdf/589502main_ITS-HBK-2810.09-02%20%5bNASA%20Information%20Security%20Incident%20Management%5d.pdf#page=9

incident

incident-disposition:incident="confirmed"

Confirmed

The incident is confirmed and response is underway following incident response procedure of the organisation.

incident-disposition:incident="deferred"

Deferred

The incident is deferred due to resource constraints, information type or external reasons.

incident-disposition:incident="unidentified"

Unidentified

The incident is unidentified because some assets, ressources or context is missing to go a state which can be handled following the incident response response procedure.

incident-disposition:incident="transferred"

Transferred

The incident is transferred to another organisations for further processing or incident handling.

incident-disposition:incident="discarded"

Discarded

The incident is discarded due to resource constraints, information type or external reasons.

incident-disposition:incident="silently-discarded"

Silently discarded

The incident is silently discarded due to resource constraints, information type or external reasons.

not-an-incident

incident-disposition:not-an-incident="insufficient-data"

Insufficient data

When insufficient data is available to explain an ambiguous (i.e., not definitively hostile or benign) indicator, the incident may be dispositioned as Insufficient Data.

incident-disposition:not-an-incident="faulty-indicator"

Faulty indicator

A false positive where an investigation reveals that the source indicator used as the basis for incident detection was a Faulty Indicator.

incident-disposition:not-an-incident="misconfiguration"

Misconfiguration

A false positive where an event that appeared to be malicious activity was subsequently disproven and determined to be a Misconfiguration (malfunction) of a system.

incident-disposition:not-an-incident="scan-probe"

Scan or Probe

Reconnaissance activity which Scanned or Probed for the presence of a vulnerability which may be later exploited to gain unauthorized access.

incident-disposition:not-an-incident="failed"

Failed

A Failed attempt to gain unauthorized access, conduct a denial of service, install malicious code, or misuse an IT resource, typically because a security control prevented it from succeeding.

incident-disposition:not-an-incident="refuted"

Refuted

Any other circumstance where a suspected incident was determined to not be an incident and was Refuted.

duplicate

incident-disposition:duplicate="duplicate"

Duplicate

An incident may be a Dup l icate of another record in the Incident Management System, and should be merged with the existing workflow.

information-security-indicators

information-security-indicators namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

A full set of operational indicators for organizations to use to benchmark their security posture.

IEX

Indicators of this category give information on the occurrence of incidents caused by external malicious threat sources.

information-security-indicators:IEX="FGY.1"

Forged domain or brand names impersonating or imitating legitimate and genuine names

Forged domains are addresses very close to the domain names legitimately filed with registration companies or organizations (forged domains are harmful only when actively used to entice customers to the website for fraudulent purposes). It also includes domain names that imitate another domain name or a brand.

information-security-indicators:IEX="FGY.2"

Wholly or partly forged websites (excluding parking pages) spoiling company’s image or business

Forged websites correspond to two main threats (forgery of sites in order to steal personal data such as account identifiers and passwords, forgery of services in order to capitalize on a brand and to generate turnover that creates unfair competition). In this case, reference is often made to phishing (1st usage) or pharming.

information-security-indicators:IEX="SPM.1"

Not requested received bulk messages (spam) targeting organization’s registered users

Spam are messages received in company’s or organization’s messaging systems in the framework of mass and not individualized campaigns, luring into clicking dangerous URLs (possibly Trojan laden) or enticing to carry out harmful to concerned individual actions.

information-security-indicators:IEX="PHI.1"

Phishing targeting company’s customers' workstations spoiling company’s image or business

Phishing involves a growing number of business sectors (financial organizations, e-commerce sites, online games, social sites etc.). It includes attacks via e-mail with messages that contain either malicious URL links (to forged websites) or malicious URL links (to malware laden genuine websites).

information-security-indicators:IEX="PHI.2"

Spear phishing or whaling carried out using social engineering and targeting organization’s specific registered users

Spear phishing are "spoofed" and customized messages looking like a usual professional relationship or an authority, and asking to click on or open dangerous URL links or dangerous attachments (malware laden).

information-security-indicators:IEX="INT.1"

Intrusion attempts on externally accessible servers

Attempts are here systematic scans (excluding network reconnaissance) and abnormal and suspicious requests on externally accessible servers, detected by an IDS/IPS or not.

information-security-indicators:IEX="INT.2"

Intrusion on externally accessible servers

Intrusion usually targets servers that host personal data (including data subject to regulations such as PCI DSS, for example). 3 objectives or motivations can be found wherever an intrusion exists: data theft (see before), installation of transfer links towards unlawful and rogue websites, getting a permanent internal access by installation of a backdoor for further purposes. This indicator does

not include the figures from the Defacement and Misappropriation indicators, both of which however starting with an intrusion. However, it includes all means and methods to get access to servers, i.e. purely technical means (such as Command execution/injection attack) or identity usurpation to log on an admin or user account (see ETSI GS ISI 002 [4] specifications).

information-security-indicators:IEX="INT.3"

Intrusions on internal servers

This kind of incident typically comes after a PC malware installation or an intrusion on an externally accessible server often followed by a lateral movement. This indicator does not include the figures from the Misappropriation indicator which may however start with an intrusion on an internal server. This indicator includes the so-called APTs (Advanced Persistent Threats), which constitute however only a small part of this indicator. APTs are long lasting and stealthy incidents with large compromises of data through outbound links, which is not the case of most incidents of the IEX_INT.3 type. This type of incident is often the result of targeted attacks.

information-security-indicators:IEX="DFC.1"

Obvious and visible websites defacements

Obvious defacements measures the defacement of homepages and of the most consulted pages of sites.

information-security-indicators:IEX="MIS.1"

Servers resources misappropriation by external attackers

This indicator measures the amount of resources of servers misappropriated by an external attacker after a successful intrusion (on an externally accessible or an internal server).

information-security-indicators:IEX="DOS.1"

Denial of service attacks on websites

This indicator measures denial-of-service attacks against websites, carried out either by sending of harmful requests (DoS), by sending a massive flow coming from multiple distributed sites (DDoS) or via other techniques. Due to the current state of the art of attack detection, the indicator is limited to DDoS attacks.

information-security-indicators:IEX="MLW.1"

Attempts to install malware on workstations

Malware installation attempts are detected by current conventional means (Antivirus and base IPS) and blocked by the same means. This indicator (which includes desktop and laptop PC based workstations, but does not include the different types of other workstations and mobile smart devices) provides an approximate insight into the malicious external pressure suffered in this regard. This indicator should be associated with indicator on successful malware installation in

order to assess the actual effectiveness of conventional detection and blockage means in the fight against malware.

information-security-indicators:IEX="MLW.2"

Attempts to install malware on servers

Malware installation attempts are detected by current conventional means (antivirus and base IPS) and blocked by the same means. This indicator gives an approximate insight into the malicious external pressure suffered in this regard. This indicator should be associated with indicator on successful malware installation in order to assess the actual effectiveness of conventional detection and blockage means in the fight against malware.

information-security-indicators:IEX="MLW.3"

Malware installed on workstations

Malware could be not detected by conventional means (lack of activation or appropriate update), or noninventoried and/or specific very stealthy incidents, most of the time not detectable by conventional means (AV and standard IPS), consequently requiring other supplementary detection means (network or WS load, outbound links, advanced network devices as DPI tools, users themselves reporting to help desks). This indicator (which includes desktop and laptop Windows-based workstations, but does not include the different types of other workstations and mobile smart devices) therefore applies to both classical viruses and worms, as well as all new malware such as Trojan horses (which are defined as malware meant to data theft or malicious transactions) or bots (which are defined here as vectors for spam or DDoS attacks).

information-security-indicators:IEX="MLW.4"

Malware installed on internal servers

Malware could be not detected by conventional means (lack of activation or of appropriate update), or noninventoried and/or specific very stealthy incidents, most of the time not detectable by conventional means (AV and standard IPS), consequently requiring other supplementary detection means (network or server load, outbound links, advanced network devices as DPI tools, administrators themselves). This indicator therefore applies to both classical viruses and worms, as well as all new malware such as Trojan horses (which are defined as malware meant to data theft or malicious transactions)

information-security-indicators:IEX="PHY.1"

Human intrusion into the organization’s perimeter

This indicator measures illicit entrance of individuals into security perimeter.

IMF

Indicators of this category provides information on the occurrence of incidents caused by malfunctions, breakdowns or human errors.

information-security-indicators:IMF="BRE.1"

Workstations accidental breakdowns or malfunctions

Breakdowns or malfunctions apply to both hardware and software, caused by system errors (components failure or bugs).

information-security-indicators:IMF="BRE.2"

Servers accidental breakdowns or malfunctions

Breakdowns or malfunctions apply to both hardware and software, caused by system errors (components failure or bugs).

information-security-indicators:IMF="BRE.3"

Mainframes accidental breakdowns or malfunctions

Breakdowns or malfunctions apply to both hardware and software, caused by system errors (components failure or bugs).

information-security-indicators:IMF="BRE.4"

Networks accidental breakdowns or malfunctions

Breakdowns or malfunctions apply to both hardware and software, caused by system errors (components failure or bugs).

information-security-indicators:IMF="MDL.1"

Delivery of email to wrong recipient

This indicator measures errors from the sender when selecting or typing email addresses leading to misdelivery incidents. Consequences may be very serious when confidentiality is critical.

information-security-indicators:IMF="LOM.1"

Loss (or theft) of mobile devices belonging to the organization

This indicator measures the loss of all types of systems containing sensitive or not information belonging to the organization, whether encrypted or not (laptop computers, USB tokens, CD-ROMs, diskettes, magnetic tapes, smartphones, tablets, etc.). In some cases, it could be difficult to differentiate losses from thefts.

information-security-indicators:IMF="LOG.1"

Downtime or malfunction of the log production function with possible legal impact

This type of event could have two main causes: an accidental system malfunction or a system manipulation error by an administrator. Logs taken into account here are systems logs and

applications logs of all servers.

information-security-indicators:IMF="LOG.2"

Absence of possible tracking of the person involved in a security event with possible legal impact

Concerns unique data related to a given and known to organization user (identifier tied to application software or directory). This indicator is a sub-set of indicator IMF_LOG.1.

information-security-indicators:IMF="LOG.3"

Downtime or malfunction of the log production function for recordings with evidential value for access to or handling of information that, at this level, is subject to law or regulatory requirements

This indicator primarily relates to Personal Identifiable Information (PII) protected by privacy laws, to information falling under the PCI-DSS regulation, to information falling under European regulation in the area of breach notification (Telcos and ISPs to begin with), and to information about electronic exchanges between employees and the exterior (electronic messaging and Internet connection). This indicator does not include possible difficulties pertaining to proof forwarding from field operations to governance (state-of-the-art unavailable). This indicator is a sub-set of indicator IMF_LOG.1, but can be identical to this one in advanced organizations.

IDB

Indicators of this category provide information on the occurrence of incidents regarding internal deviant behaviours (including especially usurpation of rights or of identity).

information-security-indicators:IDB="UID.1"

User impersonation

A person within the organization impersonates a registered user (employee, partner, contractor, external service provider) using identifier, passwords or authentication devices that had previously been obtained in an illicit manner (using a social engineering technique or not). This measures cases of usurpation for malicious purposes, and not ones that relate to user-friendly usage. Moreover, assumption is made that ID/Password is the main way of authentication

information-security-indicators:IDB="RGH.1"

Privilege escalation by exploitation of software or configuration vulnerability on an externally accessible server

Exploited vulnerabilities are typically tied to the underlying OS that supports the Web application, exploited notably through injection of additional characters in URL links. This behaviour specifically involves external service providers and company’s business partners that wish to access additional information or to launch unlawful actions (for example, service providers seeking information about their competitors). This type of behaviour is less frequent amongst employees, since it is often easier to get the same results by means of social engineering methods.

information-security-indicators:IDB="RGH.2"

Privilege escalation on a server or central application by social engineering

It is often easier to get the same results by means of social engineering methods than with technical means. Help desk teams are often involved in this kind of behaviour.

information-security-indicators:IDB="RGH.3"

```
Use on a server or central application of administrator rights illicitly granted by an
administrator
```

Illicitly granting administrator privileges generally comes from simple errors or more worrisome negligence on the part of the administrators (malicious action is rarer). The case of forgotten temporary rights (see next indicator), is not included in this indicator.

information-security-indicators:IDB="RGH.4"

Use on a server or central application of time-limited granted rights after the planned period

This indicator measures situations where time-limited user accounts (created for training, problem resolution, emergency access, test, etc.) are still in use after the initial planned period.

information-security-indicators:IDB="RGH.5"

Abuse of privileges by an administrator on a server or central application

The motivation of rights usurpation by an administrator is often the desire to breach the confidentiality of sensitive data (for example, human resources data). This indicator is similar to the indicator IDB_RGH.6 (but with consequences that may be however often potentially more serious).

information-security-indicators:IDB="RGH.6"

Abuse of privileges by an operator or a plain user on a server or central application

This indicator applies for example to authorized users having access to personal identifiable information aboutcelebrities with no real need for their job (thereby violating the "right to know").

information-security-indicators:IDB="RGH.7"

Illicit use on a server or central application of rights not removed after departure or position change within the organization

This indicator also takes into account the problem of generic accounts (whose password might have been changed each time a user knowing this password is leaving organization).

information-security-indicators:IDB="MIS.1"

Server resources misappropriation by an internal source

This indicators measures misappropriation of on-line IT resources for one’s own use (personal, association etc.).

information-security-indicators:IDB="IAC.1"

Access to hacking Website

This indicator measures unauthorized access to a hacking Website from an internal workstation

information-security-indicators:IDB="LOG.1"

Deactivating of logs recording by an administrator

This event is generally decided and deployed by an administrator in order to improve performance of the system under his/her responsibility (illicit voluntary stoppage). This indicator is a reduced subset of indicator IUS_RGH.5

IWH

Indicators of this category are indicators that concern all categories of incidents.

information-security-indicators:IWH="VNP.1"

Exploitation of a software vulnerability without available patch

This indicators measures security incidents that are the result of an exploitation of a disclosed software vulnerability that has no available patch (with or without an applied workaround measure). It is used to assess the intensity of the exploitation of recently disclosed software vulnerabilities (zero day or not). Patching here applies only to standard software (excluding bespoke software), and the scope is limited to workstations (OS, browsers and various add-ons and plug-ins, office automation standard software).

information-security-indicators:IWH="VNP.2"

Exploitation of a non-patched software vulnerability

This indicators measures security incidents that are the result of the exploitation of a non-patched software vulnerability though a patch exists. It is used to assess effectiveness or application of patching-related organization and processes and tools (patching not launched). It is linked with indicator VOR_VNP.2 that is intended to assess problems of exceeding the "time limit for the window of exposure to risks". It has the same limitations as IWH_VNP.1 regarding scope.

information-security-indicators:IWH="VNP.3"

Exploitation of a poorly-patched software vulnerability

This indicator measures security incidents that are the result of the exploitation of a poorly patched software vulnerability. It is used to assess effectiveness of patching-related organization and processes and tools (process launched but patch not operational - Cf. no reboot, etc.). It is linked with indicator VOR_VNP.1, IWH_VNP.1 and IWH_VNP.2. It has the same limitations as IWH_VNP.1 regarding scope.

information-security-indicators:IWH="VCN.1"

Exploitation of a configuration flaw

This indicator measures security incidents that are the result of the exploitation of a configuration flaw on servers or workstations. A configuration flaw should be considered as a nonconformity against state-of-the-art security policy.

information-security-indicators:IWH="UKN.1"

Not categorized security incidents

This indicator measures all types of incidents that are new and/or a complex combination of more basic incidents and cannot be fully qualified and therefore precisely categorized.

information-security-indicators:IWH="UNA.1"

Security incidents on non-inventoried and/or not managed assets

This indicator measures security incidents tied to assets (on servers) non-inventoried and not managed by appointed teams. It is a key indicator insofar as a high percentage of incidents corresponds with this indicator on average in the profession (according to some public surveys).

VBH

Indicators of this category apply to the existence of abnormal behaviours that could lead to security incidents.

information-security-indicators:VBH="PRC.1"

Server accessed by an administrator with unsecure protocols

This indicator measures the use of insecure protocols set up by an administrator to get access to organizationbased externally accessible servers making an external intrusion possible. Insecure protocol means unencrypted, without time-out, with poor authentication means etc. (for example Telnet).

information-security-indicators:VBH="PRC.2"

P2P client in a workstation

This indicator measures the installation of P2P clients set up by a user on its professional workstation with the risk of partial or full sharing of the workstation content. It applies to

workstations that are either connected to the organization's network from within the organization or directly connected to the public network from outside (notably home). There is a high risk of accidental sharing (in one quarter of all cases) of files that may host confidential company data. It is most often carried out through HTTP channel (proposed on all of these services).

information-security-indicators:VBH="PRC.3"

VoIP clients in a workstation

This indicator measures VoIP clients installed by a user on his/hers own workstation in order to use a peer-to-peer service. It applies to workstations connected to an organization's network from within the organization or directly connected to the public network from outside (notably home). The associated risk is to exchange dangerous Office documents. It is most often carried out through HTTP channel (proposed on all of these services).

information-security-indicators:VBH="PRC.4"

Outbound connection dangerously set up

This indicator measures outbound connection dangerously set up to get remote access to the company's internal network without using an inbound VPN link and a focal access point with possible exploitation by an external intruder. The outbound connection method consists for example in using a GoToMyPC™ software or a LogMeIn® software or a computer to computer connection in tunnel mode.

information-security-indicators:VBH="PRC.5"

Not compliant laptop computer used to establish a connection

This indicator measures remote or local connection to the organization's internal network from a roaming laptop computer that is organization-owned and is configured with weak parameters. In this situation and in case of the existence of a software to check compliance of roaming computers, another related software blocks the connection in principle and prevents its continuation.

information-security-indicators:VBH="PRC.6"

Other unsecure protocols used

This indicator measures other unsecure or dangerous protocols set up with similar behaviours. The other cases are the other than the 5 previous ones (VBH_PRC.1 to VBH_PRC.5). It relates to dangerous or abusive usages, i.e. situations where usages are not required and where other more secure solutions exist.

information-security-indicators:VBH="IAC.1"

Outbound controls bypassed to access Internet

This indicator measures the detection of Internet access from the internal network by means that bypass the outbound security devices. It primarily relates to Internet accesses from a perimeter

area or to tunnelling (SSL port 443) or to straight accesses (via an ADSL link or public Wi-Fi access points and the telephone network) or to accesses via Smartphones connected to the workstation. The main underlying motivation is to prevent user tracking.

information-security-indicators:VBH="IAC.2"

Anonymization site used to access Internet

This indicator measures the detection of anonymous Internet access from an internal workstation through an anonymization site. The goal is to maintain free access and to avoid organization's filtering of accesses to forbidden websites.

information-security-indicators:VBH="FTR.1"

Files recklessly downloaded

This indicator measures the download of files from an external website that is not known (no reputation) within the profession to an internal workstation. "No reputation" can be assessed by information provided by URL outbound filtering devices.

information-security-indicators:VBH="FTR.2"

Personal public instant messaging account used for business file exchanges

This indicator measures the use of personal public instant messaging accounts for business exchanges with outside. This file exchange method has to be avoided due to network AV software bypassing and to identify lesser effectiveness of AV software.

information-security-indicators:VBH="FTR.3"

Personal public messaging account used for business file exchanges

This indicator measures the use of personal public messaging accounts for business file exchanges with the exterior. The risk is to expose information to external attackers.

information-security-indicators:VBH="WTI.1"

Workstations accessed in administrator mode

This indicator measures access to workstations in administrator mode without authorization.

information-security-indicators:VBH="WTI.2"

Personal storage devices used

This indicator measures the use personal storage devices on a professional workstation to input or output information or software. Mobile or removable personal storage devices include USB tokens, smartphones, tablets, etc. It is not applicable to personal devices authorized by security policy (Cf. VBH_WTI.3 and BYOD).

information-security-indicators:VBH="WTI.3"

Personal devices used without compartmentalization (BYOD)

This indicator measures the lack of or the removal of basic security measures meant to compartmentalize professional activities on personal devices. Personal devices (BYOD) include PCs, tablets, smartphones, etc.

information-security-indicators:VBH="WTI.4"

Not encrypted sensitive files exported

This indicator measures the lack of encryption of sensitive files uploaded from a professional workstation to professional mobile or removable storage devices.

information-security-indicators:VBH="WTI.5"

Personal software used

This indicator measures the presence of personal software on a professional workstation that does not comply with the corporate security policy. It corresponds with all types of local unauthorized software (with a user licence or not), such as common personal software (games, office automation etc.) or more dangerous ones (hacking etc.). It should be added that VBH_PRC.2 and VBH_PRC.3 are a share of this indicator, and that this indicator is a subset of VBH_WTI.1.

information-security-indicators:VBH="WTI.6"

Mailbox or Internet access with admin mode

This indicator applies to users using their admin account on a workstation.to access their own mailbox or Internet. This behaviour is particularly dangerous since malware (through attached pieces on email or drive-by download on Web browser) are far easier to install on the workstation in this case.

information-security-indicators:VBH="PSW.1"

Weak passwords used

The required strength of passwords depends on the organization’s security policy, but usable general recommendations in ISO/IEC 27002 [2].

information-security-indicators:VBH="PSW.2"

Passwords not changed

This indicators measures password not changed in due periodic time (case of changes not periodically imposed). Situations in which changes are not periodically imposed by accessed systems themselves remain fairly frequent within organizations (apart from Active Directory), the figure being around 25 % of the cases on average.

information-security-indicators:VBH="PSW.3"

Administrator passwords not changed

This indicators measures password not changed in due periodic time by an administrator in charge of an account used by automated applications and processes (case of changes not periodically imposed). Situations in which changes are not periodically imposed by accessed systems themselves remain fairly frequent within organizations (apart from Active Directory), the figure being around 25 % of the cases on average.

information-security-indicators:VBH="RGH.1"

Not compliant user rights granted illicitly by an administrator

This indicator measures the granting of not compliant user rights by an administrator outside any official procedure. This vulnerability may originate with an error, negligence or malice.

information-security-indicators:VBH="HUW.1"

Human weakness exploited by a spear phishing message meant to entice or appeal to do something possibly harmful to the organization

This vulnerability typically includes clicking on an Internet link or opening an attached document

information-security-indicators:VBH="HUW.2"

```
Human weakness exploited by exchanges meant to entice or appeal to tell some secrets
to be used later
```

This vulnerability applies to discussions through on-line media leading to leakage of personal identifiable information (PII) or various business details to be used later (notably for identity usurpation)

VSW

Indicators of this category apply to the existence of weaknesses in software that could be exploited and lead to security incidents.

information-security-indicators:VSW="WSR.1"

Web applications software vulnerabilities

This indicators measures software vulnerabilities detected in Web applications running on externally accessible servers.

information-security-indicators:VSW="OSW.1"

OS software vulnerabilities regarding servers

This indicators measures software vulnerabilities detected in OS running on externally accessible servers.

information-security-indicators:VSW="WBR.1"

Web browsers software vulnerabilities

This indicators measures software vulnerabilities detected in Web browsers running on workstations.

VCF

Indicators of this category apply to the existence of weaknesses in the configuration of IT devices that could be exploited and lead to security incidents.

information-security-indicators:VCF="DIS.1"

Dangerous or illicit services on externally accessible servers

This indicator measures the presence of illicit and dangerous system services running on an externally accessible server.

information-security-indicators:VCF="LOG.1"

Insufficient size of the space allocated for logs

Such event could cause an overflow in case of quick series of unusual actions.

information-security-indicators:VCF="FWR.1"

Weak firewall filtering rules

This indicator measures the gaps between the active firewall filtering rules and the security policy.

information-security-indicators:VCF="WTI.1"

Workstation wrongly configured

This indicator measures the use of workstation with a disabled or lacking update AV and/or FW. The lack of update includes signature file older than x days (generally at least 6 days).

information-security-indicators:VCF="WTI.2"

Autorun feature enabled on workstations

This indicator measures the presence of Autorun feature enabled on workstations.

information-security-indicators:VCF="UAC.1"

Access rights configuration not compliant with the security policy

This indicator measures access rights configuration that are not compliant with corporate security policy. This indicator is more reliable in case of existence of a central repository of user rights within organization (and of an IAM achievement)

information-security-indicators:VCF="UAC.2"

Not compliant access rights on logs

This indicator measures non-compliant access rights on logs in servers which are sensitive and/or subject to regulations. This situation representing a key weakness since the necessary high confidence in the produced logs has been reduced to nothing. This indicator is a subset of VCF_UAC.1.

information-security-indicators:VCF="UAC.3"

Generic and shared administrator accounts

This indicator measures generic and shared administration accounts that are unnecessary or accounts that are necessary but without patronage. It concerns operating systems, databases and applications.

information-security-indicators:VCF="UAC.4"

Accounts without owners

This indicator measures accounts without owners that have not been erased. These are accounts that have no more assigned users (for example after internal transfer or departure of the users from organization).

information-security-indicators:VCF="UAC.5"

Inactive accounts

This indicator measures accounts inactive for at least 2 months that have not been disabled. These accounts are not used by their users due to prolonged but not definitive absence (long term illness, maternity, etc.), with the exclusion of messaging accounts (which should remain accessible to users from their home).

VTC

Indicators of this category measure the existence of weaknesses in the IT and physical architecture that could be exploited and lead to security incidents.

information-security-indicators:VTC="BKP.1"

Malfunction of server-hosted sensitive data safeguards

On servers hosting sensitive data with respect to availability, it concerns malfunctions of safeguards due to lack of periodic testing. This kind of event may be very serious since usually put trust is betrayed in a critical function.

information-security-indicators:VTC="IDS.1"

Full unavailability of IDS/IPS

Many causes are possible, including deliberate disconnection by a network administrator (to streamline operations or since IDS/IPS output is deemed too difficult to use), unwitting disconnection (error by a network administrator), breakdown, software malfunction, etc.

information-security-indicators:VTC="WFI.1"

Wi-Fi devices installed on the network without any official authorization

Many causes are possible, including for example local decisions for easier access of mobile users, rogue user behaviours or workstations configured as access points.

information-security-indicators:VTC="RAP.1"

Remote access points used to gain unauthorized access

This indicator is interesting to assess whether such accesses are localized (local areas, countries, etc.) or involve the whole organization or are increasing and spreading to whole organization.

information-security-indicators:VTC="NRG.1"

Devices or servers connected to the organization’s network without being registered and managed

According to some convergent studies, this event may be at the origin of some 70 % of all security incidents associated to malice.

information-security-indicators:VTC="PHY.1"

Not operational physical access control means

This indicator includes access to protected internal areas. The 1st cause is the lack of effective control of users at software level. The 2nd cause is hardware breakdown of a component in the chain.

VOR

Indicators of this category measure the existence of weaknesses in the organization that could be exploited and lead to security incidents.

information-security-indicators:VOR="DSC.1"

Discovery of attacks

This indicator measures stealthy security incidents difficult to detect. As most studies show, the time to discovery is often several months, time frame especially used to steal sensitive data. Incidents taken into account here are IEX_INT.3, IEX_MLW.3 and IEX_MLW.4. This indicator give landmarks regarding what may be deemed excessive, i.e. with an assumption which is above one week.

information-security-indicators:VOR="VNP.1"

Excessive time of window of risk exposure

This indicator measures situations in which the time of the window of risk exposure exceeds the time limit expressed in security policy. The window of risks exposure is the period of time between the public disclosure of a software vulnerability and the actual and checked application of a patch that corresponds with the vulnerability's remediation (independently of the time needed for the vendor to provide the patch). This indicator only applies to workstations (OS, application software and browsers), and to critical vulnerabilities (as publicly determined via the CVSS scale) that require an action as quickly as possible.

information-security-indicators:VOR="VNP.2"

Rate of not patched systems

This indicator measures the rate of not patched systems for detected critical software vulnerabilities (see VOR_VNP.1 for criticality definition). Not patched systems to be taken into account are the ones which are not patched beyond the time limit defined in security policy. This indicator only applies to workstations (OS, application software and browsers).

information-security-indicators:VOR="VNR.1"

Rate of not reconfigured systems

This indicator measures the rate of not reconfigured systems for detected critical configuration vulnerabilities. Configuration vulnerabilities are either non-conformities relative to a level 3 security policy, or discrepancies relative to a state-of-the-art available within the profession (and that can correspond with a configuration master produced by a vendor and applied within the organization). This indicator only applies to workstations (OS, application software and browsers). Not reconfigured systems to be taken into account are the ones which are not reconfigured beyond the time limit defined in security policy.

information-security-indicators:VOR="RCT.1"

Reaction plans launched without experience feedback

This indicator applies to plans for responding to incidents formalized in security policy launched without experience feedback.

information-security-indicators:VOR="RCT.2"

Reaction plans unsuccessfully launched

This indicator measures failure in the performance of plans, leading to non-recovery of incidents and to subsequent possible launch of an escalation procedure.

information-security-indicators:VOR="PRT.1"

Launch of new IT projects without information classification

This indicator measures the launch of new IT projects without information classification. Availability of a classification model and scheme within the organization would make easier this task.

information-security-indicators:VOR="PRT.2"

Launch of new specific IT projects without risk analysis

This indicator measures the launch of new specific IT projects without performing a full risk analysis.

information-security-indicators:VOR="PRT.3"

```
Launch of new IT projects of a standard type without identification of vulnerabilities
and threats
```

This indicator measures the launch of new IT projects of a standard type without identification of vulnerabilities and threats and of related security measures. For these IT projects, potential implementation of a simplified risk analysis method or of pre-defined security profiles can be applied.

IMP

Indicators as regards impact measurement.

information-security-indicators:IMP="COS.1"

Average cost to tackle a critical security incident

The average cost taken into account includes the following kinds of overhead: disruption to business operations (increased operating costs, etc.), fraud (money, etc.) and incident recovery costs (technical individual time, asset replacement, etc.). It does not include possible (generally very heavy) breach notification costs to customers and enforcement bodies (according to US and recently EU laws or regulations).

information-security-indicators:IMP="TIM.1"

Average time of Websites downtime due to whole security incidents

Applies to all 4 classes, but main security incidents concerned are malfunctions or breakdowns (software or hardware), DoS or DDoS attacks and Website defacements.

information-security-indicators:IMP="TIM.2"

Average time of Websites downtime due to successful malicious attacks

This indicator is a subset of the previous one (IMP_TIM.1) focusing on 3 possible classes (IEX, IUS, IMD).

information-security-indicators:IMP="TIM.3"

Average time of Websites downtime due to malfunctions or unintentional security incidents

This indicator is a subset of IMP_TIM.1 focusing on one class (IMF).

kill-chain

kill-chain namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

The Cyber Kill Chain, a phase-based model developed by Lockheed Martin, aims to help categorise and identify the stage of an attack.

Reconnaissance

kill-chain:Reconnaissance

Research, identification and selection of targets, often represented as crawling Internet websites such as conference proceedings and mailing lists for email addresses, social relationships, or information on specific technologies.

Weaponization

kill-chain:Weaponization

Coupling a remote access trojan with an exploit into a deliverable payload, typically by means of an automated tool (weaponizer). Increasingly, client application data files such as Adobe Portable Document Format (PDF) or Microsoft Office documents serve as the weaponized deliverable.

Delivery

kill-chain:Delivery

Transmission of the weapon to the targeted environment. The three most prevalent delivery vectors for weaponized payloads by APT actors, as observed by the Lockheed Martin Computer Incident Response Team (LM-CIRT) for the years 2004-2010, are email attachments, websites, and USB removable media.

Exploitation

kill-chain:Exploitation

After the weapon is delivered to victim host, exploitation triggers intruders' code. Most often, exploitation targets an application or operating system vulnerability, but it could also more simply exploit the users themselves or leverage an operating system feature that auto-executes code.

Installation

kill-chain:Installation

Installation of a remote access trojan or backdoor on the victim system allows the adversary to maintain persistence inside the environment.

Command and Control

kill-chain:Command and Control

Typically, compromised hosts must beacon outbound to an Internet controller server to establish a C2 channel. APT malware especially requires manual interaction rather than conduct activity automatically. Once the C2 channel establishes, intruders have 'hands on the keyboard' access inside the target environment.

Actions on Objectives

kill-chain:Actions on Objectives

Only now, after progressing through the first six phases, can intruders take actions to achieve their original objectives. Typically, this objective is data exfiltration which involves collecting, encrypting and extracting information from the victim environment; violations of data integrity or availability are potential objectives as well. Alternatively, the intruders may only desire access to the initial victim box for use as a hop point to compromise additional systems and move laterally inside the network.

malware_classification

malware_classification namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Classification based on different categories. Based on https://www.sans.org/reading-room/whitepapers/incident/malware-101-viruses-32848

malware-category

malware_classification:malware-category="Virus"

Virus

malware_classification:malware-category="Worm"

Worm

malware_classification:malware-category="Trojan"

Trojan

malware_classification:malware-category="Ransomware"

Ransomware

malware_classification:malware-category="Rootkit"

Rootkit

malware_classification:malware-category="Downloader"

Downloader

malware_classification:malware-category="Adware"

Adware

malware_classification:malware-category="Spyware"

Spyware

malware_classification:malware-category="Botnet"

Botnet

obfuscation-technique

malware_classification:obfuscation-technique="no-obfuscation"

No obfuscation is used

malware_classification:obfuscation-technique="encryption"

encryption

malware_classification:obfuscation-technique="oligomorphism"

oligomorphism

malware_classification:obfuscation-technique="metamorphism"

metamorphism

malware_classification:obfuscation-technique="stealth"

stealth

malware_classification:obfuscation-technique="armouring"

armouring

malware_classification:obfuscation-technique="tunneling"

tunneling

malware_classification:obfuscation-technique="XOR"

XOR

malware_classification:obfuscation-technique="BASE64"

BASE64

malware_classification:obfuscation-technique="ROT13"

ROT13

payload-classification

malware_classification:payload-classification="no-payload"

No payload

malware_classification:payload-classification="non-destructive"

Non-Destructive

malware_classification:payload-classification="destructive"

Destructive

malware_classification:payload-classification="dropper"

Dropper

memory-classification

malware_classification:memory-classification="resident"

In memory

malware_classification:memory-classification="temporary-resident"

In memory temporarily

malware_classification:memory-classification="swapping-mode"

Only a part loaded in memory temporarily

malware_classification:memory-classification="non-resident"

Not in memory

malware_classification:memory-classification="user-process"

As a user level process

malware_classification:memory-classification="kernel-process"

As a process in the kernel

misp

misp namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

MISP taxonomy to infer with MISP behavior or operation.

ui

misp:ui="hide"

tag to hide from the user-interface.

api

misp:api="hide"

tag to hide from the API.

expansion

Expansion tag incluencing the MISP behavior using expansion modules

misp:expansion="block"

block

contributor

misp:contributor="pgpfingerprint"

OpenPGP Fingerprint

confidence-level

misp:confidence-level="completely-confident"

Completely confident

Associated numerical value="100"

misp:confidence-level="usually-confident"

Usually confident

Associated numerical value="75"

misp:confidence-level="fairly-confident"

Fairly confident

Associated numerical value="50"

misp:confidence-level="rarely-confident"

Rarely confident

Associated numerical value="25"

misp:confidence-level="unconfident"

Unconfident

misp:confidence-level="confidence-cannot-be-evalued"

Confidence cannot be evaluated

threat-level

misp:threat-level="no-risk"

No risk

Harmless information. (CEUS threat level)

misp:threat-level="low-risk"

Low risk

Low risk which can include mass-malware. (CEUS threat level)

Associated numerical value="25"

misp:threat-level="medium-risk"

Medium risk

Medium risk which can include targeted attacks (e.g. APT). (CEUS threat level)

Associated numerical value="50"

misp:threat-level="high-risk"

High risk

High risk which can include highly sophisticated attacks or 0-day attack. (CEUS threat level)

Associated numerical value="100"

automation-level

Exclusive flag set which means the values or predicate below must be set exclusively.

misp:automation-level="unsupervised"

Generated automatically without human verification

Associated numerical value="100"

misp:automation-level="reviewed"

Generated automatically but verified by a human

Associated numerical value="50"

misp:automation-level="manual"

Output of human analysis

should-not-sync

Event with this tag should not be synced to other MISP instances

tool

Tool associated with the information taggged

misp:tool="misp2stix"

misp2stix

ms-caro-malware

ms-caro-malware namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Malware Type and Platform classification based on Microsoft's implementation of the Computer Antivirus Research Organization (CARO) Naming Scheme and Malware Terminology. Based on https://www.microsoft.com/en-us/security/portal/mmpc/shared/malwarenaming.aspx, https://www.microsoft.com/security/portal/mmpc/shared/glossary.aspx, https://www.microsoft.com/security/portal/mmpc/shared/objectivecriteria.aspx, and http://www.caro.org/definitions/index.html. Malware families are extracted from Microsoft SIRs since 2008 based on https://www.microsoft.com/security/sir/archive/default.aspx and https://www.microsoft.com/en-us/security/portal/threat/threats.aspx. Note that SIRs do NOT include all Microsoft malware families.

malware-type

ms-caro-malware:malware-type="Adware"

Adware - Software that shows you extra promotions that you cannot control as you use your PC

ms-caro-malware:malware-type="Backdoor"

A type of trojan that gives a malicious hacker access to and control of your PC

ms-caro-malware:malware-type="Behavior"

A type of detection based on file actions that are often associated with malicious activity

ms-caro-malware:malware-type="BroswerModifier"

A program than makes changes to your Internet browser without your permission

ms-caro-malware:malware-type="Constructor"

A program that can be used to automatically create malware files

ms-caro-malware:malware-type="DDoS"

When a number of PCs are made to access a website, network or server repeatedly within a given time period. The aim of the attack is to overload the target so that it crashes and can’t respond

ms-caro-malware:malware-type="Dialer"

A program that makes unauthorized telephone calls. These calls may be charged at a premium rate and cost you a lot of money

ms-caro-malware:malware-type="DoS"

When a target PC or server is deliberately overloaded so that it doesn’t work for any visitors anymore

ms-caro-malware:malware-type="Exploit"

A piece of code that uses software vulnerabilities to access information on your PC or install malware

ms-caro-malware:malware-type="HackTool"

A type of tool that can be used to allow and maintain unauthorized access to your PC

ms-caro-malware:malware-type="Joke"

A program that pretends to do something malicious but actually doesn't actually do anything harmful. For example, some joke programs pretend to delete files or format disks

ms-caro-malware:malware-type="Misleading"

The program that makes misleading or fraudulent claims about files, registry entries or other items on your PC

ms-caro-malware:malware-type="MonitoringTool"

A commercial program that monitors what you do on your PC. This can include monitoring what keys you press; your email or instant messages; your voice or video conversations; and your banking details and passwords. It can also take screenshots as you use your PC

ms-caro-malware:malware-type="Program"

Software that you may or may not want installed on your PC

ms-caro-malware:malware-type="PUA"

Potentially Unwanted Applications. Characteristics of unwanted software can include depriving users of adequate choice or control over what the software does to the computer, preventing users from removing the software, or displaying advertisements without clearly identifying their source.

ms-caro-malware:malware-type="PWS"

A type of malware that is used steal your personal information, such as user names and passwords. It often works along with a keylogger that collects and sends information about what keys you press and websites you visit to a malicious hacker

ms-caro-malware:malware-type="Ransom"

A detection for malicious programs that seize control of the computer on which they are installed. This trojan usually locks the screen and prevents the user from using the computer. It usually displays an alert message.

ms-caro-malware:malware-type="RemoteAccess"

A program that gives someone access to your PC from a remote location. This type of program is often installed by the computer owner

ms-caro-malware:malware-type="Rogue"

Software that pretends to be an antivirus program but doesn't actually provide any security. This type of software usually gives you a lot of alerts about threats on your PC that don't exist. It also tries to convince you to pay for its services

ms-caro-malware:malware-type="SettingsModifier"

A program that changes your PC settings

ms-caro-malware:malware-type="SoftwareBundler"

A program that installs unwanted software on your PC at the same time as the software you are trying to install, without adequate consent

ms-caro-malware:malware-type="Spammer"

A trojan that sends large numbers of spam emails. It may also describe the person or business responsible for sending spam

ms-caro-malware:malware-type="Spoofer"

A type of trojan that makes fake emails that look like they are from a legitimate source

ms-caro-malware:malware-type="Spyware"

A program that collects your personal information, such as your browsing history, and uses it without adequate consent

ms-caro-malware:malware-type="Tool"

A type of software that may have a legitimate purpose, but which may also be abused by malware authors

ms-caro-malware:malware-type="Trojan"

A trojan is a program that tries to look innocent, but is actually a malicious application. Unlike a virus or a worm , a trojan doesn’t spread by itself. Instead they try to look innocent to convince you to download and install them. Once installed, a trojan can steal your personal information, download more malware, or give a malicious hacker access to your PC

ms-caro-malware:malware-type="TrojanClicker"

A type of trojan that can use your PC to click on websites or applications. They are usually used to make money for a malicious hacker by clicking on online advertisements and making it look like the website gets more traffic than it does. They can also be used to skew online polls, install programs on your PC, or make unwanted software appear more popular than it is

ms-caro-malware:malware-type="TrojanDownloader"

A type of trojan that installs other malicious files, including malware, onto your PC. It can download the files from a remote PC or install them directly from a copy that is included in its file.

ms-caro-malware:malware-type="TrojanDropper"

A type of trojan that installs other malicious files, including malware, onto your PC. It can download the files from a remote PC or install them directly from a copy that is included in its file.

ms-caro-malware:malware-type="TrojanNotifier"

A type of trojan that sends information about your PC to a malicious hacker. It is similar to a password stealer

ms-caro-malware:malware-type="TrojanProxy"

A type of trojan that installs a proxy server on your PC. The server can be configured so that when you use the Internet, any requests you make are sent through a server controlled by a malicious hacker.

ms-caro-malware:malware-type="TrojanSpy"

A program that collects your personal information, such as your browsing history, and uses it without adequate consent.

ms-caro-malware:malware-type="VirTool"

A detection that is used mostly for malware components, or tools used for malware-related actions, such as rootkits.

ms-caro-malware:malware-type="Virus"

A type of malware. Viruses spread on their own by attaching their code to other programs, or copying themselves across systems and networks.

ms-caro-malware:malware-type="Worm"

A type of malware that spreads to other PCs. Worms may spread using one or more of the following methods: Email programs, Instant messaging programs, File-sharing programs, Social networking sites, Network shares, Removable drives with Autorun enabled, Software vulnerabilities

malware-platform

ms-caro-malware:malware-platform="AndroidOS"

Android operating system

ms-caro-malware:malware-platform="DOS"

MS-DOS platform

ms-caro-malware:malware-platform="EPOC"

Psion devices

ms-caro-malware:malware-platform="FreeBSD"

FreeBSD platform

ms-caro-malware:malware-platform="iPhoneOS"

iPhone operating system

ms-caro-malware:malware-platform="Linux"

Linux platform

ms-caro-malware:malware-platform="MacOS"

MAC 9.x platform or earlier

ms-caro-malware:malware-platform="MacOS_X"

MacOS X or later

ms-caro-malware:malware-platform="OS2"

OS2 platform

ms-caro-malware:malware-platform="Palm"

Palm operating system

ms-caro-malware:malware-platform="Solaris"

System V-based Unix platforms

ms-caro-malware:malware-platform="SunOS"

Unix platforms 4.1.3 or earlier

ms-caro-malware:malware-platform="SymbOS"

Symbian operatings system

ms-caro-malware:malware-platform="Unix"

General Unix platforms

ms-caro-malware:malware-platform="Win16"

Win16 (3.1) platform

ms-caro-malware:malware-platform="Win2K"

Windows 2000 platform

ms-caro-malware:malware-platform="Win32"

Windows 32-bit platform

ms-caro-malware:malware-platform="Win64"

Windows 64-bit platform

ms-caro-malware:malware-platform="Win95"

Windows 95, 98 and ME platforms

ms-caro-malware:malware-platform="Win98"

Windows 98 platform only

ms-caro-malware:malware-platform="WinCE"

Windows CE platform

ms-caro-malware:malware-platform="WinNT"

WinNT

ms-caro-malware:malware-platform="ABAP"

Advanced Business Application Programming scripts

ms-caro-malware:malware-platform="ALisp"

ALisp scripts

ms-caro-malware:malware-platform="AmiPro"

AmiPro script

ms-caro-malware:malware-platform="ANSI"

American National Standards Institute scripts

ms-caro-malware:malware-platform="AppleScript"

compiled Apple scripts

ms-caro-malware:malware-platform="ASP"

Active Server Pages scripts

ms-caro-malware:malware-platform="AutoIt"

AutoIT scripts

ms-caro-malware:malware-platform="BAS"

Basic scripts

ms-caro-malware:malware-platform="BAT"

Basic scripts

ms-caro-malware:malware-platform="CorelScript"

Corelscript scripts

ms-caro-malware:malware-platform="HTA"

HTML Application scripts

ms-caro-malware:malware-platform="HTML"

HTML Application scripts

ms-caro-malware:malware-platform="INF"

Install scripts

ms-caro-malware:malware-platform="IRC"

mIRC/pIRC scripts

ms-caro-malware:malware-platform="Java"

Java binaries (classes)

ms-caro-malware:malware-platform="JS"

Javascript scripts

ms-caro-malware:malware-platform="LOGO"

LOGO scripts

ms-caro-malware:malware-platform="MPB"

MapBasic scripts

ms-caro-malware:malware-platform="MSH"

Monad shell scripts

ms-caro-malware:malware-platform="MSIL"

ms-caro-malware:malware-platform="Perl"

Net intermediate language scripts
Perl scripts

ms-caro-malware:malware-platform="PHP"

Hypertext Preprocessor scripts

ms-caro-malware:malware-platform="Python"

Python scripts

ms-caro-malware:malware-platform="SAP"

SAP platform scripts

ms-caro-malware:malware-platform="SH"

Shell scripts

ms-caro-malware:malware-platform="VBA"

Visual Basic for Applications scripts

ms-caro-malware:malware-platform="VBS"

Visual Basic scripts

ms-caro-malware:malware-platform="WinBAT"

Winbatch scripts

ms-caro-malware:malware-platform="WinHlp"

Windows Help scripts

ms-caro-malware:malware-platform="WinREG"

Windows registry scripts

ms-caro-malware:malware-platform="A97M"

Access 97, 2000, XP, 2003, 2007, and 2010 macros

ms-caro-malware:malware-platform="HE"

macro scripting

ms-caro-malware:malware-platform="O97M"

Office 97, 2000, XP, 2003, 2007, and 2010 macros - those that affect Word, Excel, and Powerpoint

ms-caro-malware:malware-platform="PP97M"

PowerPoint 97, 2000, XP, 2003, 2007, and 2010 macros

ms-caro-malware:malware-platform="V5M"

Visio5 macros

ms-caro-malware:malware-platform="W1M"

Word1Macro

ms-caro-malware:malware-platform="W2M"

Word2Macro

ms-caro-malware:malware-platform="W97M"

Word 97, 2000, XP, 2003, 2007, and 2010 macros

ms-caro-malware:malware-platform="WM"

Word 95 macros

ms-caro-malware:malware-platform="X97M"

Excel 97, 2000, XP, 2003, 2007, and 2010 macros

ms-caro-malware:malware-platform="XF"

Excel formulas

ms-caro-malware:malware-platform="XM"

Excel 95 macros

ms-caro-malware:malware-platform="ASX"

XML metafile of Windows Media .asf files

ms-caro-malware:malware-platform="HC"

HyperCard Apple scripts

ms-caro-malware:malware-platform="MIME"

MIME packets

ms-caro-malware:malware-platform="Netware"

Novell Netware files

ms-caro-malware:malware-platform="QT"

Quicktime files

ms-caro-malware:malware-platform="SB"

StarBasic (Staroffice XML) files

ms-caro-malware:malware-platform="SWF"

Shockwave Flash files

ms-caro-malware:malware-platform="TSQL"

MS SQL server files

ms-caro-malware:malware-platform="XML"

XML files

ms-caro-malware-full

ms-caro-malware-full namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Malware Type and Platform classification based on Microsoft's implementation of the Computer Antivirus Research Organization (CARO) Naming Scheme and Malware Terminology. Based on https://www.microsoft.com/en-us/security/portal/mmpc/shared/malwarenaming.aspx, https://www.microsoft.com/security/portal/mmpc/shared/glossary.aspx, https://www.microsoft.com/security/portal/mmpc/shared/objectivecriteria.aspx, and http://www.caro.org/definitions/index.html. Malware families are extracted from Microsoft SIRs since 2008 based on https://www.microsoft.com/security/sir/archive/default.aspx and https://www.microsoft.com/en-us/security/portal/threat/threats.aspx. Note that SIRs do NOT include all Microsoft malware families.

malware-type

ms-caro-malware-full:malware-type="Adware"

Adware - Software that shows you extra promotions that you cannot control as you use your PC

ms-caro-malware-full:malware-type="Backdoor"

A type of trojan that gives a malicious hacker access to and control of your PC

ms-caro-malware-full:malware-type="Behavior"

A type of detection based on file actions that are often associated with malicious activity

ms-caro-malware-full:malware-type="BroswerModifier"

A program than makes changes to your Internet browser without your permission

ms-caro-malware-full:malware-type="Constructor"

A program that can be used to automatically create malware files

ms-caro-malware-full:malware-type="DDoS"

When a number of PCs are made to access a website, network or server repeatedly within a given time period. The aim of the attack is to overload the target so that it crashes and can't respond

ms-caro-malware-full:malware-type="Dialer"

A program that makes unauthorized telephone calls. These calls may be charged at a premium rate and cost you a lot of money

ms-caro-malware-full:malware-type="DoS"

When a target PC or server is deliberately overloaded so that it doesn't work for any visitors

anymore

ms-caro-malware-full:malware-type="Exploit"

A piece of code that uses software vulnerabilities to access information on your PC or install malware

ms-caro-malware-full:malware-type="HackTool"

A type of tool that can be used to allow and maintain unauthorized access to your PC

ms-caro-malware-full:malware-type="Joke"

A program that pretends to do something malicious but actually doesn't actually do anything harmful. For example, some joke programs pretend to delete files or format disks

ms-caro-malware-full:malware-type="Misleading"

The program that makes misleading or fraudulent claims about files, registry entries or other items on your PC

ms-caro-malware-full:malware-type="MonitoringTool"

A commercial program that monitors what you do on your PC. This can include monitoring what keys you press; your email or instant messages; your voice or video conversations; and your banking details and passwords. It can also take screenshots as you use your PC

ms-caro-malware-full:malware-type="Program"

Software that you may or may not want installed on your PC

ms-caro-malware-full:malware-type="PUA"

Potentially Unwanted Applications. Characteristics of unwanted software can include depriving users of adequate choice or control over what the software does to the computer, preventing users from removing the software, or displaying advertisements without clearly identifying their source.

ms-caro-malware-full:malware-type="PWS"

A type of malware that is used steal your personal information, such as user names and passwords. It often works along with a keylogger that collects and sends information about what keys you press and websites you visit to a malicious hacker

ms-caro-malware-full:malware-type="Ransom"

A detection for malicious programs that seize control of the computer on which they are installed. This trojan usually locks the screen and prevents the user from using the computer. It usually displays an alert message.

ms-caro-malware-full:malware-type="RemoteAccess"

A program that gives someone access to your PC from a remote location. This type of program is often installed by the computer owner

ms-caro-malware-full:malware-type="Rogue"

Software that pretends to be an antivirus program but doesn't actually provide any security. This type of software usually gives you a lot of alerts about threats on your PC that don't exist. It also tries to convince you to pay for its services

ms-caro-malware-full:malware-type="SettingsModifier"

A program that changes your PC settings

ms-caro-malware-full:malware-type="SoftwareBundler"

A program that installs unwanted software on your PC at the same time as the software you are trying to install, without adequate consent

ms-caro-malware-full:malware-type="Spammer"

A trojan that sends large numbers of spam emails. It may also describe the person or business responsible for sending spam

ms-caro-malware-full:malware-type="Spoofer"

A type of trojan that makes fake emails that look like they are from a legitimate source

ms-caro-malware-full:malware-type="Spyware"

A program that collects your personal information, such as your browsing history, and uses it without adequate consent

ms-caro-malware-full:malware-type="Tool"

A type of software that may have a legitimate purpose, but which may also be abused by malware authors

ms-caro-malware-full:malware-type="Trojan"

A trojan is a program that tries to look innocent, but is actually a malicious application. Unlike a virus or a worm , a trojan doesn't spread by itself. Instead they try to look innocent to convince you to download and install them. Once installed, a trojan can steal your personal information, download more malware, or give a malicious hacker access to your PC

ms-caro-malware-full:malware-type="TrojanClicker"

A type of trojan that can use your PC to click on websites or applications. They are usually used to

make money for a malicious hacker by clicking on online advertisements and making it look like the website gets more traffic than it does. They can also be used to skew online polls, install programs on your PC, or make unwanted software appear more popular than it is

ms-caro-malware-full:malware-type="TrojanDownloader"

A type of trojan that installs other malicious files, including malware, onto your PC. It can download the files from a remote PC or install them directly from a copy that is included in its file.

ms-caro-malware-full:malware-type="TrojanDropper"

A type of trojan that installs other malicious files, including malware, onto your PC. It can download the files from a remote PC or install them directly from a copy that is included in its file.

ms-caro-malware-full:malware-type="TrojanNotifier"

A type of trojan that sends information about your PC to a malicious hacker. It is similar to a password stealer

ms-caro-malware-full:malware-type="TrojanProxy"

A type of trojan that installs a proxy server on your PC. The server can be configured so that when you use the Internet, any requests you make are sent through a server controlled by a malicious hacker.

ms-caro-malware-full:malware-type="TrojanSpy"

A program that collects your personal information, such as your browsing history, and uses it without adequate consent.

ms-caro-malware-full:malware-type="VirTool"

A detection that is used mostly for malware components, or tools used for malware-related actions, such as rootkits.

ms-caro-malware-full:malware-type="Virus"

A type of malware. Viruses spread on their own by attaching their code to other programs, or copying themselves across systems and networks.

ms-caro-malware-full:malware-type="Worm"

A type of malware that spreads to other PCs. Worms may spread using one or more of the following methods: Email programs, Instant messaging programs, File-sharing programs, Social networking sites, Network shares, Removable drives with Autorun enabled, Software vulnerabilities

malware-platform

ms-caro-malware-full:malware-platform="AndroidOS"

Android operating system

ms-caro-malware-full:malware-platform="DOS"

MS-DOS platform

ms-caro-malware-full:malware-platform="EPOC"

Psion devices

ms-caro-malware-full:malware-platform="FreeBSD"

FreeBSD platform

ms-caro-malware-full:malware-platform="iPhoneOS"

iPhone operating system

ms-caro-malware-full:malware-platform="Linux"

Linux platform

ms-caro-malware-full:malware-platform="MacOS"

MAC 9.x platform or earlier

ms-caro-malware-full:malware-platform="MacOS_X"

MacOS X or later

ms-caro-malware-full:malware-platform="OS2"

OS2 platform

ms-caro-malware-full:malware-platform="Palm"

Palm operating system

ms-caro-malware-full:malware-platform="Solaris"

System V-based Unix platforms

ms-caro-malware-full:malware-platform="SunOS"

Unix platforms 4.1.3 or earlier

ms-caro-malware-full:malware-platform="SymbOS"

Symbian operatings system

ms-caro-malware-full:malware-platform="Unix"

General Unix platforms

ms-caro-malware-full:malware-platform="Win16"

Win16 (3.1) platform

ms-caro-malware-full:malware-platform="Win2K"

Windows 2000 platform

ms-caro-malware-full:malware-platform="Win32"

Windows 32-bit platform

ms-caro-malware-full:malware-platform="Win64"

Windows 64-bit platform

ms-caro-malware-full:malware-platform="Win95"

Windows 95, 98 and ME platforms

ms-caro-malware-full:malware-platform="Win98"

Windows 98 platform only

ms-caro-malware-full:malware-platform="WinCE"

Windows CE platform

ms-caro-malware-full:malware-platform="WinNT"

WinNT

ms-caro-malware-full:malware-platform="ABAP"

Advanced Business Application Programming scripts

ms-caro-malware-full:malware-platform="ALisp"

ALisp scripts

ms-caro-malware-full:malware-platform="AmiPro"

AmiPro script

ms-caro-malware-full:malware-platform="ANSI"

American National Standards Institute scripts

ms-caro-malware-full:malware-platform="AppleScript"

compiled Apple scripts

ms-caro-malware-full:malware-platform="ASP"

Active Server Pages scripts

ms-caro-malware-full:malware-platform="AutoIt"

AutoIT scripts

ms-caro-malware-full:malware-platform="BAS"

Basic scripts

ms-caro-malware-full:malware-platform="BAT"

Basic scripts

ms-caro-malware-full:malware-platform="CorelScript"

Corelscript scripts

ms-caro-malware-full:malware-platform="HTA"

HTML Application scripts

ms-caro-malware-full:malware-platform="HTML"

HTML Application scripts

ms-caro-malware-full:malware-platform="INF"

Install scripts

ms-caro-malware-full:malware-platform="IRC"

mIRC/pIRC scripts

ms-caro-malware-full:malware-platform="Java"

Java binaries (classes)

ms-caro-malware-full:malware-platform="JS"

Javascript scripts

ms-caro-malware-full:malware-platform="LOGO"

LOGO scripts

ms-caro-malware-full:malware-platform="MPB"

MapBasic scripts

ms-caro-malware-full:malware-platform="MSH"

Monad shell scripts

ms-caro-malware-full:malware-platform="MSIL"

ms-caro-malware-full:malware-platform="Perl"

Net intermediate language scripts
Perl scripts

ms-caro-malware-full:malware-platform="PHP"

Hypertext Preprocessor scripts

ms-caro-malware-full:malware-platform="Python"

Python scripts

ms-caro-malware-full:malware-platform="SAP"

SAP platform scripts

ms-caro-malware-full:malware-platform="SH"

Shell scripts

ms-caro-malware-full:malware-platform="VBA"

Visual Basic for Applications scripts

ms-caro-malware-full:malware-platform="VBS"

Visual Basic scripts

ms-caro-malware-full:malware-platform="WinBAT"

Winbatch scripts

ms-caro-malware-full:malware-platform="WinHlp"

Windows Help scripts

ms-caro-malware-full:malware-platform="WinREG"

Windows registry scripts

ms-caro-malware-full:malware-platform="A97M"

Access 97, 2000, XP, 2003, 2007, and 2010 macros

ms-caro-malware-full:malware-platform="HE"

macro scripting

ms-caro-malware-full:malware-platform="O97M"

Office 97, 2000, XP, 2003, 2007, and 2010 macros - those that affect Word, Excel, and Powerpoint

ms-caro-malware-full:malware-platform="PP97M"

PowerPoint 97, 2000, XP, 2003, 2007, and 2010 macros

ms-caro-malware-full:malware-platform="V5M"

Visio5 macros

ms-caro-malware-full:malware-platform="W1M"

Word1Macro

ms-caro-malware-full:malware-platform="W2M"

Word2Macro

ms-caro-malware-full:malware-platform="W97M"

Word 97, 2000, XP, 2003, 2007, and 2010 macros

ms-caro-malware-full:malware-platform="WM"

Word 95 macros

ms-caro-malware-full:malware-platform="X97M"

Excel 97, 2000, XP, 2003, 2007, and 2010 macros

ms-caro-malware-full:malware-platform="XF"

Excel formulas

ms-caro-malware-full:malware-platform="XM"

Excel 95 macros

ms-caro-malware-full:malware-platform="ASX"

XML metafile of Windows Media .asf files

ms-caro-malware-full:malware-platform="HC"

HyperCard Apple scripts

ms-caro-malware-full:malware-platform="MIME"

MIME packets

ms-caro-malware-full:malware-platform="Netware"

Novell Netware files

ms-caro-malware-full:malware-platform="QT"

Quicktime files

ms-caro-malware-full:malware-platform="SB"

StarBasic (Staroffice XML) files

ms-caro-malware-full:malware-platform="SWF"

Shockwave Flash files

ms-caro-malware-full:malware-platform="TSQL"

MS SQL server files

ms-caro-malware-full:malware-platform="XML"

XML files

malware-family

ms-caro-malware-full:malware-family="Zlob"

2008 - A family of trojans that often pose as downloadable media codecs. When installed, Win32/Zlob displays frequent pop-up advertisements for rogue security software

ms-caro-malware-full:malware-family="Vundo"

2008 - A multiplecomponent family of programs that deliver pop-up advertisements and may download and execute arbitrary files. Vundo is often installed as a browser helper object (BHO) without a user's consent

ms-caro-malware-full:malware-family="Virtumonde"

2008 - multi-component malware family that displays pop-up advertisements for rogue security software

ms-caro-malware-full:malware-family="Bancos"

```
2008 -  A data-stealing trojan that captures online banking credentials and relays
them to the attacker. Most variants target customers of Brazilian banks.
```

ms-caro-malware-full:malware-family="Cutwail"

2008 - A trojan that downloads and executes arbitrary files, usually to send spam. Win32/Cutwail has also been observed to transmit Win32/Newacc

ms-caro-malware-full:malware-family="Oderoor"

2008 - a backdoor trojan that allows an attacker access and control of the compromised computer. This trojan may connect with remote web sites and SMTP servers.

ms-caro-malware-full:malware-family="Newacc"

2008 - An attacker tool that automatically registers new e-mail accounts on Hotmail, AOL, Gmail, Lycos and other account service providers, using a Web service to decode CAPTCHA protection.

ms-caro-malware-full:malware-family="Captiya"

2008 - A trojan that transmits CAPTCHA images to a botnet, in what is believed to be an effort to improve the botnet's ability to detect characters and break CAPTCHAs more successfully

ms-caro-malware-full:malware-family="Taterf"

2008 - A family of worms that spread through mapped drives in order to steal login and account details for popular online games.

ms-caro-malware-full:malware-family="Frethog"

2008 - A large family of password-stealing trojans that target confidential data, such as account information, from massively multiplayer online games

ms-caro-malware-full:malware-family="Tilcun"

2008 - A family of trojans that steals online game passwords and sends this captured data to remote sites.

ms-caro-malware-full:malware-family="Ceekat"

2008 - A collection of trojans that steal information such as passwords for online games, usually by reading information directly from running processes in memory. Different variants target different processes.

ms-caro-malware-full:malware-family="Corripio"

2008 - a loosely-related family of trojans that attempt to steal passwords for popular online games. Detections containing the name Win32/Corripio are generic, and hence may be reported for a large number of different malicious password-stealing trojans that are otherwise behaviorally dissimilar.

ms-caro-malware-full:malware-family="Zuten"

2008 - A family of malware that steals information from online games.

ms-caro-malware-full:malware-family="Lolyda"

2008 - A family of trojans that sends account information from popular online games to a remote server. They may also download and execute arbitrary files.

ms-caro-malware-full:malware-family="Storark"

2008 - A family of trojans that steals online game passwords and sends this captured data to remote sites.

ms-caro-malware-full:malware-family="Renos"

2008 - A family of trojan downloaders that installs rogue security software.

ms-caro-malware-full:malware-family="ZangoSearchAssistant"

2008 - Adware that monitors the user's Web-browsing activity and displays pop-up advertisements related to the Internet sites the user is viewing.

ms-caro-malware-full:malware-family="ZangoShoppingReports"

2008 - Adware that displays targeted advertising to affected users while they browse the Internet, based on search terms entered into search engines.

ms-caro-malware-full:malware-family="FakeXPA"

2008 - A rogue security software family that claims to scan for malware and then demands that the user pay to remove nonexistent threats. Some variants unlawfully use Microsoft logos and trademarks.

ms-caro-malware-full:malware-family="FakeSecSen"

2008 - A rogue security software family that claims to scan for malware and then demands that the user pay to remove non-existent threats. It appears to be based on Win32/SpySheriff

ms-caro-malware-full:malware-family="Hotbar"

2008 - Adware that displays a dynamic toolbar and targeted pop-up ads based on its monitoring of Web-browsing activity.

ms-caro-malware-full:malware-family="Agent"

2008 - A generic detection for a number of trojans that may perform different malicious functions. The behaviors exhibited by this family are highly variable

ms-caro-malware-full:malware-family="Wimad"

2008 - A detection for malicious Windows Media files that can be used to encourage users to download and execute arbitrary files on an affected machine.

ms-caro-malware-full:malware-family="BaiduSobar"

2008 - A Chinese language Web browser toolbar that delivers pop-up and contextual advertisements, blocks certain other advertisements, and changes the Internet Explorer search page

ms-caro-malware-full:malware-family="VB"

2008 - A detection for various threats written in the Visual Basic programming language.

ms-caro-malware-full:malware-family="Antivirus2008"

2008 - A program that displays misleading security alerts in order to convince users to purchase

rogue security software. It may be installed by Win32/Renos or manually by a computer user.

ms-caro-malware-full:malware-family="Playmp3z"

2008 - An adware family that may display advertisements in connection with the use of a 'free music player' from the site 'PlayMP3z.biz.'

ms-caro-malware-full:malware-family="Tibs"

2008 - a family of Trojans that may download and run other malicious software or may steal user data and send it to the attacker via HTTP POST or email. The Win32/Tibs family frequently downloads Trojans belonging to the Win32/Harnig and Win32/Passalert families, both of which are families of Trojan downloaders which may in turn download and run other malicious software

ms-caro-malware-full:malware-family="SeekmoSearchAssistant"

2008 - Adware that displays targeted search results and pop-up advertisements based on terms that the user enters for Web searches. The pop-up advertisements may include adult content.

ms-caro-malware-full:malware-family="RJump"

2008 - a worm that attempts to spread by copying itself to newly attached media (such as USB memory devices or network drives). It also contains backdoor functionality that allows an attacker unauthorized access to an affected computer

ms-caro-malware-full:malware-family="SpywareSecure"

2008 - A program that displays misleading warning messages in order to convince users to purchase a product that removes spyware

ms-caro-malware-full:malware-family="Winfixer"

2008 - A program that locates various registry entries, Windows prefetch content, and other types of data, identifies them as privacy violations, and urges the user to purchase the product to fix them.

ms-caro-malware-full:malware-family="C2Lop"

2008 - a trojan that modifies Web browser settings, adds Web browser bookmarks to advertisements, updates itself and delivers pop-up and contextual advertisements.

ms-caro-malware-full:malware-family="Matcash"

2008 - a multicomponent family of trojans that downloads and executes arbitrary files. Some variants of this family may install a toolbar. observed to use the Win32/Slenfbot worm as a means of distribution.

ms-caro-malware-full:malware-family="Horst"

2008 - CAPTCHA Breaker typically delivered through an executable application that masquerades as an illegal software crack or key generator

ms-caro-malware-full:malware-family="Slenfbot"

2008 - A family of worms that can spread via instant messaging programs, and may spread via removable drives. They also contain backdoor functionality that allows unauthorized access to an affected machine. This worm does not spread automatically upon installation but must be ordered to spread by a remote attacker.

ms-caro-malware-full:malware-family="Rustock"

2008 - A multicomponent family of rootkitenabled backdoor trojans, developed to aid in the distribution of spam. Recent variants appear to be associated with the incidence of rogue security programs.

ms-caro-malware-full:malware-family="Gimmiv"

2008 - a family of trojans that are sometimes installed by exploits of a vulnerability documented in Microsoft Security Bulletin MS08-067.

ms-caro-malware-full:malware-family="Yektel"

2008 - A family of trojans that display fake warnings of spyware or malware in an attempt to lure the user into installing or paying money to register rogue security products such as Win32/FakeXPA.

ms-caro-malware-full:malware-family="Roron"

2008 - This virus spreads by attaching its code to other files on your PC or network. Some of the infected programs might no longer run correctly. Attempts to send personal information to a remote address. It may spread via e-mail, network shares, or peer-to-peer file sharing.

ms-caro-malware-full:malware-family="Swif"

2008 - A trojan that exploits a vulnerability in Adobe Flash Player to download malicious files. Adobe has published security bulletin APSB08-11 addressing the vulnerability.

ms-caro-malware-full:malware-family="Mult"

2008 - A group of threats, written in JavaScript, that attempt to exploit multiple vulnerabilities on affected computers in order to download, execute or otherwise run arbitrary code. The malicious JavaScript may be hosted on compromised or malicious websites, embedded in specially crafted PDF files, or could be called by other malicious scripts.

ms-caro-malware-full:malware-family="Wukill"

2008 - a family of mass-mailing e-mail and network worms. The Win32/Wukill worm spreads to root directories on certain local and mapped drives. The worm also spreads by sending a copy of itself as an attachment to e-mail addresses found on the infected computer.

ms-caro-malware-full:malware-family="Objsnapt"

2008 - A detection for a Javascript file that exploits a known vulnerability in the Microsoft Access Snapshot Viewer ActiveX Control.

ms-caro-malware-full:malware-family="Redirector"

2008 - The threat is a piece of JavaScript code that is inserted on bad or hacked websites. It can direct your browser to a website you don’t want to go to. You might see the detection for this threat if you visit a bad or hacked website, or if you open an email message.

ms-caro-malware-full:malware-family="Xilos"

2008 - a detection for a proof-of-concept JavaScript obfuscation technique, which was originally published in 2002 in the sixth issue of 29A, an early online magazine for virus creators

ms-caro-malware-full:malware-family="Decdec"

2008 - A detection for certain malicious JavaScript code injected in HTML pages. The virus will execute on user computers that visit compromised websites.

ms-caro-malware-full:malware-family="BearShare"

2008 - A P2P file-sharing client that uses the decentralized Gnutella network. Free versions of BearShare have come bundled with advertising supported and other potentially unwanted software.

ms-caro-malware-full:malware-family="BitAccelerator"

2008 - A program that redirects Web search results to other Web sites and may display various advertisements to users while browsing Web sites.

ms-caro-malware-full:malware-family="Blubtool"

2008 - An Internet browser search toolbar that may be installed by other third-party software, such as a peer-to-peer file sharing application. It may modify Internet explorer search settings and display unwanted advertisements.

ms-caro-malware-full:malware-family="RServer"

2008 - Commercial remote administration software that can be used to control a computer. These programs are typically installed by the computer owner or administrator and should only be removed if unexpected

ms-caro-malware-full:malware-family="UltraVNC"

2008 - A remote access program that can be used to control a computer. This program is typically installed by the computer owner or administrator, and should only be removed if unexpected.

ms-caro-malware-full:malware-family="GhostRadmin"

2008 - A remote administration tool that can be used to control a computer. These programs are typically installed by the computer owner or administrator and should only be removed if unexpected

ms-caro-malware-full:malware-family="TightVNC"

2008 - A remote control program that allows full control of the computer. These programs are typically installed by the computer owner or administrator and should only be removed if unexpected

ms-caro-malware-full:malware-family="DameWareMiniRemoteControl"

2008 - A detection for the DameWare Mini Remote Control tools. This program was detected by definitions prior to 1.147.1889.0 as it violated the guidelines by which Microsoft identified unwanted software. Based on analysis using current guidelines, the program does not have unwanted behaviors. Microsoft has released definition 1.147.1889.0 which no longer detects this program.

ms-caro-malware-full:malware-family="SeekmoSearchAssistant_Repack"

2008 - A detection that is triggered by modified (that is, edited and re-packed) remote control programs based on DameWare Mini Remote Control, a commercial software product

ms-caro-malware-full:malware-family="Nbar"

2008 - A program that may display advertisements and redirect user searches to a certain website. It may also download malicious or unwanted content into the system without user consent.

ms-caro-malware-full:malware-family="Chir"

2008 - A family with a worm component and a virus component. The worm component spreads by email and by exploiting a vulnerability addressed by Microsoft Security Bulletin MS01-020. The virus component may infect .exe, .scr, and HTML files.

ms-caro-malware-full:malware-family="Sality"

2008 - A family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.

ms-caro-malware-full:malware-family="Obfuscator"

2008 - A detection for programs that use a combination of obfuscation techniques to hinder analysis or detection by antivirus scanners

ms-caro-malware-full:malware-family="ByteVerify"

2008 - a detection of malicious code that attempts to exploit a vulnerability in the Microsoft Virtual Machine (VM). This flaw enables attackers to execute arbitrary code on a user's machine such as writing, downloading and executing additional malware. This vulnerability is addressed by update MS03-011, released in 2003.

ms-caro-malware-full:malware-family="Autorun"

2008 - A family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.

ms-caro-malware-full:malware-family="Hamweq"

2008 - A worm that spreads through removable drives, such as USB memory sticks. It may contain an IRC-based backdoor enabling the computer to be controlled remotely by an attacker

ms-caro-malware-full:malware-family="Brontok"

2008 - a family of mass-mailing e-mail worms. The worm spreads by sending a copy of itself as an e-mail attachment to e-mail addresses that it gathers from files on the infected computer. It can also copy itself to USB and pen drives. Win32/Brontok can disable antivirus and security software, immediately terminate certain applications, and cause Windows to restart immediately when certain applications run. The worm may also conduct denial of service (DoS) attacks against certain Web sites

ms-caro-malware-full:malware-family="SpywareProtect"

2008 - A rogue security software family that may falsely claim that the user's computer is infected and encourages the user to buy a product for cleaning the alleged malware from the computer

ms-caro-malware-full:malware-family="Cbeplay"

2008 - A trojan that may upload computer operating system details to a remote Web site, download additional malware, and terminate debugging utilities

ms-caro-malware-full:malware-family="InternetAntivirus"

2008 - A program that displays false and misleading malware alerts to convince users to purchase rogue security software. This program also displays a fake Windows Security Center message

ms-caro-malware-full:malware-family="Nuwar"

2008 - A family of trojan droppers that install a distributed P2P downloader trojan. This

downloader trojan in turn downloads an e-mail worm component.

ms-caro-malware-full:malware-family="Rbot"

2008 - A family of backdoor trojans that allows attackers to control the computer through an IRC channel

ms-caro-malware-full:malware-family="IRCbot"

2008 - A large family of backdoor trojans that drops malicious software and connects to IRC servers via a backdoor to receive commands from attackers.

ms-caro-malware-full:malware-family="SkeemoSearchAssistant"

2008 - A program that displays targeted search results and pop-up advertisements based on terms that the user enters for Web searches. The pop-up advertisements may include adult content

ms-caro-malware-full:malware-family="RealVNC"

2008 - A management tool that allows a computer to be controlled remotely. It can be installed for legitimate purposes, but can also be installed from a remote location by an attacker.

ms-caro-malware-full:malware-family="MoneyTree"

2008 - A family of software that provides the ability to search for adult content on local disk. It may also install other potentially unwanted software, such as programs that display pop-up ads.

ms-caro-malware-full:malware-family="Tracur"

2008 - A trojan that downloads and executes arbitrary files. It is sometimes distributed by ASX/Wimad.

ms-caro-malware-full:malware-family="Meredrop"

2008 - This is a generic detection for trojans that install and run malware on your PC. These trojans have been deliberately created in a complex way to hide their purpose and make them difficult to analyze.

ms-caro-malware-full:malware-family="Banker"

2008 - A family of data-stealing trojans that captures banking credentials such as account numbers and passwords from computer users and relays them to the attacker. Most variants target customers of Brazilian banks; some variants target customers of other banks.

ms-caro-malware-full:malware-family="Ldpinch"

2008 - a family of password-stealing trojans. This trojan gathers private user data such as passwords from the host computer and sends the data to the attacker at a preset e-mail address. The Win32/Ldpinch trojans use their own Simple Mail Transfer Protocol (SMTP) engine or a web-

based proxy for sending the e-mail, thus copies of the sent e-mail will not appear in the affected user's e-mail client.

ms-caro-malware-full:malware-family="Advantage"

2008 - a family of adware that displays pop-up advertisements and contacts a remote server to download updates

ms-caro-malware-full:malware-family="Parite"

2008 - a family of polymorphic file infectors that targets computers running Microsoft Windows. The virus infects .exe and .scr executable files on the local file system and on writeable network shares. In turn, the infected executable files perform operations that cause other .exe and .scr files to become infected.

ms-caro-malware-full:malware-family="PossibleHostsFileHijack"

2008 - an indicator that the computer's HOSTS file may have been modified by malicious or potentially unwanted software

ms-caro-malware-full:malware-family="Alureon"

2008 - A data-stealing trojan that gathers confidential information such as user names, passwords, and credit card data from incoming and outgoing Internet traffic. It may also download malicious data and modify DNS settings.

ms-caro-malware-full:malware-family="PowerRegScheduler"

2008 - This program was detected by definitions prior to 1.159.567.0 as it violated the guidelines by which Microsoft identified unwanted software. Based on analysis using current guidelines, the program does not have unwanted behaviors. Microsoft has released definition 1.159.567.0 which no longer detects this program.

ms-caro-malware-full:malware-family="APSB08-11"

2008 - A trojan that attempts to exploit a vulnerability in Adobe Flash Player. In the wild, this trojan has been used to download and execute arbitrary files, including other malware.

ms-caro-malware-full:malware-family="ConHook"

2008 - A family of Trojans that installs themselves as Browser Helper Objects (BHOs), and connects to the Internet without user consent. They also terminate specific security services, and download additional malware to the computer.

ms-caro-malware-full:malware-family="Starware"

2008 - This program was detected by definitions prior to 1.159.567.0 as it violated the guidelines by which Microsoft identified unwanted software. Based on analysis using current guidelines, the program does not have unwanted behaviors. Microsoft has released definition 1.159.567.0 which no

longer detects this program.

ms-caro-malware-full:malware-family="WinSpywareProtect"

2008 - A program that may falsely claim that the user's system is infected and encourages the user to buy a promoted product for cleaning the alleged malware from the computer.

ms-caro-malware-full:malware-family="MessengerSkinner"

2008 - A program, that may be distributed in the form of a freeware application, that displays advertisements, downloads additional files, and uses stealth to hide its presence

ms-caro-malware-full:malware-family="Skintrim"

2008 - A trojan that downloads and executes arbitrary files. It may be distributed by as a Microsoft Office Outlook addon used to display emoticons or other animated icons within e-mail messages.

ms-caro-malware-full:malware-family="AdRotator"

2008 - delivers advertisements, and as the name suggests, rotates advertisements among sponsors. AdRotator contacts remote Web sites in order to deliver updated content. This application also displays fake error messages that encourage users to download and install additional applications.

ms-caro-malware-full:malware-family="Wintrim"

2008 - A family of trojans that display pop-up advertisements depending on the user's keywords and browsing history. Its variants can monitor the user's activities, download applications, and send system information back to a remote server.

ms-caro-malware-full:malware-family="Busky"

2008 - A family of Trojans that monitor and redirect Internet traffic, gather system information and download unwanted software such as Win32/Renos and Win32/SpySheriff. Win32/Busky may be installed by a Web browser exploit or other vulnerability when visiting a malicious Web site.

ms-caro-malware-full:malware-family="WhenU"

2008 - This program was detected by definitions prior to 1.173.303.0 as it violated the guidelines by which Microsoft identified unwanted software. Based on analysis using current guidelines, the program does not have unwanted behaviors.

ms-caro-malware-full:malware-family="Mobis"

2008 - This program was detected by definitions prior to 1.175.2037.0 as it violated the guidelines by which Microsoft identified unwanted software. Based on analysis using current guidelines, the program does not have unwanted behaviors.

ms-caro-malware-full:malware-family="Sogou"

2008 - Detected by definitions prior to 1.155.995.0 as it violated the guidelines by which Microsoft identified unwanted software. Based on analysis using current guidelines, the program does not have unwanted behaviors. Microsoft has released definition 1.155.995.0 which no longer detects this program.

ms-caro-malware-full:malware-family="Sdbot"

2008 - A family of backdoor trojans that allows attackers to control infected computers. After a computer is infected, the trojan connects to an internet relay chat (IRC) server and joins a channel to receive commands from attackers.

ms-caro-malware-full:malware-family="DelfInject"

2008 - This threat can download and run files on your PC.

ms-caro-malware-full:malware-family="Vapsup"

2008 - This threat can perform a number of actions of a malicious hacker’s choice on your PC.

ms-caro-malware-full:malware-family="BrowsingEnhancer"

2008 - This program was detected by definitions prior to 1.175.1834.0 as it violated the guidelines by which Microsoft identified unwanted software. Based on analysis using current guidelines, the program does not have unwanted behaviors.

ms-caro-malware-full:malware-family="Jeefo"

2008 - virus infects executable files, such as files with a .exe extension. When an infected file runs, the virus tries to run the original content of the file while it infects other executable files on your PC. This threat might have got on your PC if you inserted a removable disk or accessed a network connection that was infected.

ms-caro-malware-full:malware-family="Sezon"

2008 - An adware that redirects web browsing to advertising or search sites.

ms-caro-malware-full:malware-family="RuPass"

2008 - a DLL component which may be utilized by adware or malicious programs in order to monitor an affected user’s Internet usage and to capture sensitive information. Win32/RuPass has been distributed as a 420,352 byte DLL file, with the file name 'ConnectionServices.dll'.

ms-caro-malware-full:malware-family="OneStepSearch"

2008 - Modifies the user’s browser to deliver targeted advertisements when the user enters search keywords. It may also replace or override web browser error pages that would otherwise be displayed when unresolvable web addresses are entered into the browser’s address bar.

ms-caro-malware-full:malware-family="GameVance"

2008 - Software that displays advertisements and tracks anonymous usage information in exchange for a free online gaming experience at the Web address 'gamevance.com.'

ms-caro-malware-full:malware-family="E404"

2008 - is a browser helper object (BHO) that takes advantage of invalid or mistyped URLs entered in the address bar by redirecting the browser to Web sites containing adware

ms-caro-malware-full:malware-family="Mirar"

2008 - This program was detected by definitions prior to 1.175.2037.0 as it violated the guidelines by which Microsoft identified unwanted software. Based on analysis using current guidelines, the program does not have unwanted behaviors.

ms-caro-malware-full:malware-family="Fotomoto"

2008 - A Trojan that lowers security settings, delivers advertisements, and sends system and network configuration details to a remote Web site.

ms-caro-malware-full:malware-family="Ardamax"

2008 - The tool can capture your activity on your PC (such as the keys you press when typing in passwords) and might send this information to a hacker.

ms-caro-malware-full:malware-family="Hupigon"

2008 - A family of trojans that uses a dropper to install one or more backdoor files and sometimes installs a password stealer or other malicious programs.

ms-caro-malware-full:malware-family="CNNIC"

2008 - enables Chinese keyword searching in Internet Explorer and adds support for other applications to use Chinese domain names that registered with CNNIC. Also contains a kernel driver that protects its files and registry settings from being modified or deleted

ms-caro-malware-full:malware-family="MotePro"

2008 - May display advertisement pop-ups, and download programs from predefined Web sites. When installed, Win32/MotePro runs as a Web Browser Helper Object (BHO).

ms-caro-malware-full:malware-family="CnsMin"

2008 - Installs a browser helper object (BHO) that redirects Internet Explorer searches to a Chinese search portal. CnsMin may be installed without adequate user consent. It may prevent its files from being removed or restore files that have been previously removed.

ms-caro-malware-full:malware-family="BaiduIebar"

2008 - A detection for an address line search tool. This program was detected by definitions prior to 1.153.956.0 as it violated the guidelines by which Microsoft identified unwanted software. Based on analysis using current guidelines, the program does not have unwanted behaviors. Microsoft has released definition 1.153.956.0 which no longer detects this program.

ms-caro-malware-full:malware-family="Ejik"

2008 - This program was detected by definitions prior to 1.175.1915.0 as it violated the guidelines by which Microsoft identified unwanted software. Based on analysis using current guidelines, the program does not have unwanted behaviors.

ms-caro-malware-full:malware-family="AlibabaIEToolBar"

2008 - This program was detected by definitions prior to 1.175.1834.0 as it violated the guidelines by which Microsoft identified unwanted software. Based on analysis using current guidelines, the program does not have unwanted behaviors.

ms-caro-malware-full:malware-family="BDPlugin"

2008 - a DLL file which is usually introduced to an affected system as a component of BrowserModifier:Win32/BaiduSobar. It may display unwanted pop-ups and advertisements on the affected system.

ms-caro-malware-full:malware-family="Adialer"

2008 - A trojan dialer program that connects to a premium number, or attempts to connect to adult websites via particular phone numbers without your permission, connects to remote hosts without user consent.

ms-caro-malware-full:malware-family="EGroupSexDial"

2008 - A dialer program that may attempt to dial a premium number, thus possibly resulting in international phone charges for the user.

ms-caro-malware-full:malware-family="Zonebac"

2008 - A family of backdoor Trojans that allows a remote attacker to download and run arbitrary programs, and which may upload computer configuration information and other potentially sensitive data to remote Web sites.

ms-caro-malware-full:malware-family="Antinny"

2008 - A family of worms that targets certain versions of Microsoft Windows. The worm spreads using a Japanese peer-to-peer file-sharing application named Winny. The worm creates a copy of itself with a deceptive file name in the Winny upload folder so that it can be downloaded by other Winny users.

ms-caro-malware-full:malware-family="RewardNetwork"

2008 - A program that monitors an affected user's Internet usage and reports this usage to a remote server. Win32/RewardNetwork may be visible as an Internet Explorer toolbar.

ms-caro-malware-full:malware-family="Virut"

2008 - A family of file infecting viruses that target and infect .exe and .scr files accessed on infected systems. Win32/Virut also opens a backdoor by connecting to an IRC server

ms-caro-malware-full:malware-family="Allaple"

2008 - A multi-threaded, polymorphic network worm capable of spreading to other computers connected to a local area network (LAN) and performing denial-of-service (DoS) attacks against targeted remote Web sites.

ms-caro-malware-full:malware-family="VKit_DA"

2008 - This virus spreads by attaching its code to other files on your PC or network. Some of the infected programs might no longer run correctly.

ms-caro-malware-full:malware-family="Small"

2008 - A generic detection for a variety of threats.

ms-caro-malware-full:malware-family="Netsky"

2008 - A mass-mailing worm that spreads by e-mailing itself to addresses found on an infected computer. Some variants contain a backdoor component and perform DoS attacks.

ms-caro-malware-full:malware-family="Luder"

2008 - A virus that spreads by infecting executable files, by inserting itself into .RAR archive files, and by sending a copy of itself as an attachment to e-mail addresses found on the infected computer. This virus has a date-activated, file damaging payload, and may connect to a remote server and accept commands from an attacker.

ms-caro-malware-full:malware-family="IframeRef"

2008 - A generic detection for specially formed IFrame tags that point to remote websites that contain malicious content.

ms-caro-malware-full:malware-family="Lovelorn"

2008 - This threat is classified as a mass-mailing worm. A mass mailing email worm is self-contained malicious code that propagates by sending itself through e-mail. Typically, a mass mailing email worm uses its own SMTP engine to send itself, thus copies of the sent worm will not appear in the infected user's outgoing or sent email folders. Technical details are currently not available.

ms-caro-malware-full:malware-family="Cekar"

2008 - This threat downloads and installs other programs, including other malware, onto your PC without your consent.

ms-caro-malware-full:malware-family="Dialsnif"

2008 - This threat can perform a number of actions of a malicious hacker’s choice on your PC.

ms-caro-malware-full:malware-family="Conficker"

2008 - A worm that spreads by exploiting a vulnerability addressed by Security Bulletin MS08-067. Some variants also spread via removable drives and by exploiting weak passwords. It disables several important system services and security products and downloads arbitrary files.

ms-caro-malware-full:malware-family="LoveLetter"

2009 - A family of mass-mailing worms that targets computers running certain versions of Windows. It can spread as an e-mail attachment and through an Internet Relay Chat (IRC) channel. The worm can download, overwrite, delete, infect, and run files on the infected computer.

ms-caro-malware-full:malware-family="VBSWGbased"

2009 - A generic detection for VBScript code that is known to be automatically generated by a particular malware tool.

ms-caro-malware-full:malware-family="Slammer"

2009 - A memory resident worm that spreads through a vulnerability present in computers running either MSDE 2000 or SQL Server that have not applied Microsoft Security Bulletin MS02-039.

ms-caro-malware-full:malware-family="Msblast"

2009 - A family of network worms that exploit a vulnerability addressed by security bulletin MS03-039. The worm may attempt Denial of Service (DoS) attacks on some server sites or create a backdoor on the infected system

ms-caro-malware-full:malware-family="Sasser"

2009 - A family of network worms that exploit a vulnerability fixed by security bulletin MS04-011. The worm spreads by randomly scanning IP addresses for vulnerable machines and infecting any that are found

ms-caro-malware-full:malware-family="Nimda"

2009 - A family of worms that spread by exploiting a vulnerability addressed by Microsoft Security Bulletin MS01-020. The worm compromises security by sharing the C drive and creating a Guest account with administrator permissions.

ms-caro-malware-full:malware-family="Mydoom"

2009 - A family of massmailing worms that spread through e-mail. Some variants also spread through P2P networks. It acts as a backdoor trojan and can sometimes be used to launch DoS attacks against specific Web sites

ms-caro-malware-full:malware-family="Bagle"

2009 - A worm that spreads by e-mailing itself to addresses found on an infected computer. Some variants also spread through peer-to-peer (P2P) networks. Bagle acts as a backdoor trojan and can be used to distribute other malicious software.

ms-caro-malware-full:malware-family="Winwebsec"

2009 - A family of rogue security software programs that have been distributed with several different names. The user interface varies to reflect each variant’s individual branding

ms-caro-malware-full:malware-family="Koobface"

2009 - A multicomponent family of malware used to compromise computers and use them to perform various malicious tasks. It spreads through the internal messaging systems of popular social networking sites

ms-caro-malware-full:malware-family="Pdfjsc"

2009 - a family of specially crafted PDF files that exploits vulnerabilities in Adobe Acrobat and Adobe Reader. The files contain malicious JavaScript that executes when opened with a vulnerable program.

ms-caro-malware-full:malware-family="Pointfree"

2009 - a browser modifier that redirects users when invalid Web site addresses or search terms are entered in the Windows Internet Explorer address bar

ms-caro-malware-full:malware-family="Chadem"

2009 - A trojan that steals password details from an infected computer by monitoring network traffic associated with FTP connections.

ms-caro-malware-full:malware-family="FakeIA"

2009 - A rogue security software family that impersonates the Windows Security Center. It may display product names or logos in an apparently unlawful attempt to impersonate Microsoft products

ms-caro-malware-full:malware-family="Waledac"

2009 - A trojan that is used to send spam. It also has the ability to download and execute arbitrary files, harvest e-mail addresses from the local machine, perform denial-of-service attacks, proxy

network traffic, and sniff passwords

ms-caro-malware-full:malware-family="Provis"

2009 - This threat can perform a number of actions of a malicious hacker’s choice on your PC.

ms-caro-malware-full:malware-family="Prolaco"

2009 - A family of worms that spreads via email, removable drives, Peer-to-Peer (P2P) and network shares. This worm may also drop and execute other malware.

ms-caro-malware-full:malware-family="Mywife"

2009 - A mass-mailing network worm that targets certain versions of Microsoft Windows. The worm spreads through e-mail attachments and writeable network shares. It is designed to corrupt the content of specific files on the third day of every month.

ms-caro-malware-full:malware-family="Melissa"

2009 - A macro worm that spreads via e-mail and by infecting Word documents and templates. It is designed to work in Word 97 and Word 2000, and it uses Outlook to reach new targets through e-mail

ms-caro-malware-full:malware-family="Rochap"

2009 - A family of multicomponent trojans that download and execute additional malicious files. While downloading, some variants display a video from the Web site 'youtube.com' presumably to distract the user

ms-caro-malware-full:malware-family="Gamania"

2009 - A family of trojans that steals online game passwords and sends them to remote sites.

ms-caro-malware-full:malware-family="Mabezat"

2009 - a polymorphic virus that infects Windows executable files. Apart from spreading through file infection, it also attempts to spread through e-mail attachments, network shares, removable drives and by CD-burning. It also contains a date-based payload that encrypts files with particular extensions.

ms-caro-malware-full:malware-family="Helpud"

2009 - A family of trojans that steals login information for popular online games. The gathered information is then sent to remote websites.

ms-caro-malware-full:malware-family="PrivacyCenter"

2009 - a family of programs that claims to scan for malware and displays fake warnings of 'malicious programs and viruses'. They then inform the user that they need to pay money to

register the software in order to remove these non-existent threats.

ms-caro-malware-full:malware-family="FakeRean"

2009 - This family of rogue security programs pretend to scan your PC for malware, and often report lots of infections. The program will say you have to pay for it before it can fully clean your PC. However, the program hasn't really detected any malware at all and isn't really an antivirus or antimalware scanner. It just looks like one so you'll send money to the people who made the program. Some of these programs use product names or logos that unlawfully impersonate Microsoft products.

ms-caro-malware-full:malware-family="Bredolab"

2009 - A downloader that can access and execute arbitrary files from a remote host. Bredolab has been observed to download several other malware families to infected computers

ms-caro-malware-full:malware-family="Rugzip"

2009 - A trojan that downloads other malware from predefined Web sites. Rugzip may itself be installed by other malware. Once it has performed its malicious routines, it deletes itself to avoid detection.

ms-caro-malware-full:malware-family="Fakespypro"

2009 - A rogue security family that falsely claims that the affected computer is infected with malware and encourages the user to buy a promoted product it claims will clean the computer.

ms-caro-malware-full:malware-family="Buzuz"

2009 - A trojan that downloads malware known as 'SpywareIsolator' a rogue security software program.

ms-caro-malware-full:malware-family="PoisonIvy"

2009 - A family of backdoor trojans that allow unauthorized access to and control of an affected machine. Poisonivy attempts to hide by injecting itself into other processes

ms-caro-malware-full:malware-family="AgentBypass"

2009 - A detection for files that attempt to inject possibly malicious code into the explorer.exe process.

ms-caro-malware-full:malware-family="Enfal"

2009 - This threat can perform a number of actions of a malicious hacker's choice on your PC.

ms-caro-malware-full:malware-family="SystemHijack"

2009 - A generic detection that uses advanced heuristics in the Microsoft Antivirus engine to detect

malware that displays particular types of malicious behavior.

ms-caro-malware-full:malware-family="ProcInject"

2009 - This threat can perform a number of actions of a malicious hacker’s choice on your PC.

ms-caro-malware-full:malware-family="Malres"

2009 - A trojan that drops another malware, detected as Virtool:WinNT/Malres.A, into the system.

ms-caro-malware-full:malware-family="Kirpich"

2009 - a trojan that drops malicious code into the system. It also infects two system files; the infected files are detected as Virus:Win32/Kirpich.A, in the system. This does not constitute virus behavior for the trojan as it does not infect any other files and therefore does not have any conventional replication routines. TrojanDropper:Win32/Kirpich.A also disables Data Execution Protection and steals specific system information.

ms-caro-malware-full:malware-family="Malagent"

2009 - A generic detection for a variety of threats.

ms-caro-malware-full:malware-family="Bumat"

2009 - A generic detection for a variety of threats.

ms-caro-malware-full:malware-family="Bifrose"

2009 - A backdoor trojan that allows a remote attacker to access the compromised computer and injects its processes into the Windows shell and Internet Explorer.

ms-caro-malware-full:malware-family="Ripinip"

2009 - This threat can give a hacker unauthorized access and control of your PC.

ms-caro-malware-full:malware-family="Riler"

2009 - This threat can perform a number of actions of a malicious hacker’s choice on your PC.

ms-caro-malware-full:malware-family="Farfli"

2009 - A trojan that drops various files detected as malware into a system. It also has backdoor capabilities that allow it to contact a remote attacker and wait for instructions.

ms-caro-malware-full:malware-family="PcClient"

2009 - A backdoor trojan family with several components including a key logger, backdoor, and a rootkit.

ms-caro-malware-full:malware-family="Veden"

2009 - A name used for backdoor trojan detections that have been added to Microsoft signatures after advanced automated analysis.

ms-caro-malware-full:malware-family="Banload"

2009 - A family of trojans that download other malware. Banload usually downloads Win32/Banker, which steals banking credentials and other sensitive data and sends it back to a remote attacker.

ms-caro-malware-full:malware-family="Microjoin"

2009 - a tool that is used to deploy malware without being detected. It is used to bundle multiple files, consisting of a clean file and malware files, into a single executable.

ms-caro-malware-full:malware-family="Killav"

2009 - a trojan that terminates a large number of security-related processes, including those for antivirus, monitoring, or debugging tools, and may install certain exploits for the vulnerability addressed by Microsoft Security Bulletin MS08-067

ms-caro-malware-full:malware-family="Cinmus"

2009 - This threat can perform a number of actions of a malicious hacker’s choice on your PC.

ms-caro-malware-full:malware-family="MessengerPlus"

2009 - A non-Microsoft add-on for Microsoft’s Windows Live Messenger, called Messenger Plus!. It comes with an optional sponsor program installation, detected as Spyware:Win32/C2Lop.

ms-caro-malware-full:malware-family="Haxdoor"

2009 - a backdoor trojan that allows remote control of the machine over the Internet. The trojan is rootkit-enabled, allowing it to hide processes and files related to the threat. Haxdoor lowers security settings on the computer and gathers user and system information to send to a third party

ms-caro-malware-full:malware-family="Nieguide"

2009 - a detection for a DLL file that connects to a Web site and may display advertisements or download other programs

ms-caro-malware-full:malware-family="Ithink"

2009 - displays pop-up advertisements; it is usually bundled with other applications

ms-caro-malware-full:malware-family="Pointad"

2009 - This program was detected by definitions prior to 1.175.2145.0 as it violated the guidelines by which Microsoft identified unwanted software. Based on analysis using current guidelines, the

program does not have unwanted behaviors.

ms-caro-malware-full:malware-family="Webdir"

2009 - A Web Browser Helper Object (BHO) used to collect user information and display targeted advertisings using Internet Explorer browser. Webdir attempts to modify certain visited urls to include affiliate IDs.

ms-caro-malware-full:malware-family="Microbillsys"

2009 - a program that processes payments made to a billing Web site. It is considered potentially unwanted software because it cannot be removed from the Add/Remove Programs list in Control Panel; rather, a user requires an 'uninstall code' before the program can be removed.

ms-caro-malware-full:malware-family="Kerlofost"

2009 - a browser helper object (BHO) that may modify browsing behavior; redirect searches; report user statistics, behavior, and searches back to a remote server; and display pop-up advertisements.

ms-caro-malware-full:malware-family="Zwangi"

2009 - A program that runs as a service in the background and modifies Web browser settings to visit a particular Web site

ms-caro-malware-full:malware-family="DoubleD"

2009 - an adware program that displays pop-up advertising, runs at each system start and is installed as an Internet Explorer toolbar.

ms-caro-malware-full:malware-family="ShopAtHome"

2009 - A browser redirector that monitors Web-browsing behavior and online purchases. It claims to track points for ShopAtHome rebates when the user buys products directly from affiliated merchant Web sites.

ms-caro-malware-full:malware-family="FakeVimes"

2009 - a downloading component of Win32/FakeVimes - a family of programs that claims to scan for malware and displays fake warnings of 'malicious programs and viruses'. They then inform the user that they need to pay money to register the software in order to remove these non-existent threats.

ms-caro-malware-full:malware-family="FakeCog"

2009 - This threat claims to scan your PC for malware and then shows you fake warnings. They try to convince you to pay to register the software to remove the non-existent threats.

ms-caro-malware-full:malware-family="FakeAdPro"

2009 - a program that may display false and misleading alerts regarding errors and malware to entice users to purchase it.

ms-caro-malware-full:malware-family="FakeSmoke"

2009 - a family of trojans consisting of a fake Security Center interface and a fake antivirus program.

ms-caro-malware-full:malware-family="FakeBye"

2009 - A rogue security software family that uses a Korean-language user interface.

ms-caro-malware-full:malware-family="Hiloti"

2009 - a generic detection for a trojan that interferes with an affected user’s browsing habits and downloads and executes arbitrary files.

ms-caro-malware-full:malware-family="Tikayb"

2009 - A trojan that attempts to establish a secure network connection to various Web sites without the user’s consent.

ms-caro-malware-full:malware-family="Ursnif"

2009 - A family of trojans that steals sensitive information from an affected computer

ms-caro-malware-full:malware-family="Rimecud"

2009 - A family of worms with multiple components that spreads via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system

ms-caro-malware-full:malware-family="Lethic"

2009 - A trojan that connects to remote servers, which may lead to unauthorized access to an affected system.

ms-caro-malware-full:malware-family="CeeInject"

2009 - This threat has been 'obfuscated', which means it has tried to hide its purpose so your security software doesn’t detect it. The malware that lies underneath this obfuscation can have almost any purpose.

ms-caro-malware-full:malware-family="Cmdow"

2009 - a detection for a command-line tool and violated the guidelines by which Microsoft identified unwanted software.

ms-caro-malware-full:malware-family="Yabector"

2009 - This trojan can use your PC to click on online advertisements without your permission or knowledge. This can earn money for a malicious hacker by making a website or application appear more popular than it is.

ms-caro-malware-full:malware-family="Renocide"

2009 - a family of worms that spread via local, removable, and network drives and also using file sharing applications. They have IRC-based backdoor functionality, which may allow a remote attacker to execute commands on the affected computer.

ms-caro-malware-full:malware-family="Liften"

2009 - a trojan that is used to stop affected users from downloading security updates. It is downloaded by Trojan:Win32/FakeXPA.

ms-caro-malware-full:malware-family="ShellCode"

2009 - A generic detection for JavaScript-enabled objects that contain exploit code and may exhibit suspicious behavior. Malicious websites and malformed PDF documents may contain JavaScript that attempts to execute code without the affected user's consent.

ms-caro-malware-full:malware-family="FlyAgent"

2009 - A backdoor trojan program that is capable of performing several actions depending on the commands of a remote attacker.

ms-caro-malware-full:malware-family="Psyme"

2009 - This threat downloads and installs other programs, including other malware, onto your PC without your consent.

ms-caro-malware-full:malware-family="Orsam"

2009 - A generic detection for a variety of threats. A name used for trojans that have been added to MS signatures after advanced automated analysis.

ms-caro-malware-full:malware-family="AgentOff"

2009 - This threat can perform a number of actions of a malicious hacker's choice on your PC.

ms-caro-malware-full:malware-family="Nuj"

2009 - a worm that copies itself to fixed, removable or network drives. Some variants of this worm may also terminate antivirus-related processes.

ms-caro-malware-full:malware-family="Sohanad"

2009 - Worms automatically spread to other PCs. They can do this in a number of ways, including by copying themselves to removable drives, network folders, or spreading through email.

ms-caro-malware-full:malware-family="I2ISolutions"

2009 - This program was detected by definitions prior to 1.175.2037.0 as it violated the guidelines by which Microsoft identified unwanted software. Based on analysis using current guidelines, the program does not have unwanted behaviors.

ms-caro-malware-full:malware-family="Dpoint"

2009 - This program was detected by definitions prior to 1.175.1915.0 as it violated the guidelines by which Microsoft identified unwanted software. Based on analysis using current guidelines, the program does not have unwanted behaviors.

ms-caro-malware-full:malware-family="Silly_P2P"

2009 - Worms automatically spread to other PCs. They can do this in a number of ways, including by copying themselves to removable drives, network folders, or spreading through email.

ms-caro-malware-full:malware-family="Vobfus"

2009 - This family of worms can download other malware onto your PC, including: Win32/Beebone, Win32/Fareit, Win32/Zbot. Vobfus worms can be downloaded by other malware or spread via removable drives, such as USB flash drives.

ms-caro-malware-full:malware-family="Daurso"

2009 - a family of trojans that attempts to steal sensitive information, including passwords and FTP authentication details from affected computers. This family targets particular FTP applications and also attempts to steal data from Protected Storage.

ms-caro-malware-full:malware-family="MyDealAssistant"

2009 - This program was detected by definitions prior to 1.175.2037.0 as it violated the guidelines by which Microsoft identified unwanted software. Based on analysis using current guidelines, the program does not have unwanted behaviors.

ms-caro-malware-full:malware-family="Adsubscribe"

2009 - This program was detected by definitions prior to 1.175.1834.0 as it violated the guidelines by which Microsoft identified unwanted software. Based on analysis using current guidelines, the program does not have unwanted behaviors.

ms-caro-malware-full:malware-family="MyCentria"

2009 - This program was detected by definitions prior to 1.175.2037.0 as it violated the guidelines by

which Microsoft identified unwanted software. Based on analysis using current guidelines, the program does not have unwanted behaviors.

ms-caro-malware-full:malware-family="Fierads"

2009 - This program was detected by definitions prior to 1.175.2037.0 as it violated the guidelines by which Microsoft identified unwanted software. Based on analysis using current guidelines, the program does not have unwanted behaviors.

ms-caro-malware-full:malware-family="VBInject"

2009 - This is a generic detection for malicious files that are obfuscated using particular techniques to prevent their detection or analysis.

ms-caro-malware-full:malware-family="PerfectKeylogger"

2009 - a commercial monitoring program that monitors user activity, such as keystrokes typed. MonitoringTool:Win32/PerfectKeylogger is available for purchase at the company's website. It may also have been installed without user consent by a Trojan or other malware.

ms-caro-malware-full:malware-family="AgoBot"

2010 VOL09 - A backdoor that communicates with a central server using IRC.

ms-caro-malware-full:malware-family="Bubnix"

2010 VOL09 - A generic detection for a kernel-mode driver installed by other malware that hides its presence on an affected computer by blocking registry and file access to itself. The trojan may report its installation to a remote server and download and distribute spam email messages and could download and execute arbitrary files.

ms-caro-malware-full:malware-family="Citeary"

2010 VOL09 - A kernel mode driver installed by Win32/Citeary, a worm that spreads to all available drives including the local drive, installs device drivers and attempts to download other malware from a predefined website.

ms-caro-malware-full:malware-family="Fakeinit"

2010 VOL09 - A rogue security software family distributed under the names Internet Security 2010, Security Essentials 2010, and others.

ms-caro-malware-full:malware-family="Oficla"

2010 VOL09 - A family of trojans that attempt to inject code into running processes in order to download and execute arbitrary files. It may download rogue security programs.

ms-caro-malware-full:malware-family="Pasur"

2010 VOL09 - a name used for backdoor trojan detections that have been added to Microsoft signatures after advanced automated analysis.

ms-caro-malware-full:malware-family="PrettyPark"

2010 VOL09 - A worm that spreads via email attachments. It allows backdoor access and control of an infected computer.

ms-caro-malware-full:malware-family="Prorat"

2010 VOL09 - A trojan that opens random ports that allow remote access from an attacker to the affected computer. This backdoor may download and execute other malware from predefined websites and may terminate several security applications or services.

ms-caro-malware-full:malware-family="Pushbot"

2010 VOL09 - A detection for a family of malware that spreads via MSN Messenger, Yahoo! Messenger, and AIM when commanded by a remote attacker. It contains backdoor functionality that allows unauthorized access and control of an affected machine.

ms-caro-malware-full:malware-family="Randex"

2010 VOL09 - A worm that scans randomly generated IP addresses to attempt to spread to network shares with weak passwords. After the worm infects a computer, it connects to an IRC server to receive commands from the attacker.

ms-caro-malware-full:malware-family="SDBot"

2010 VOL09 - A family of backdoor trojans that allows attackers to control infected computers over an IRC channel.

ms-caro-malware-full:malware-family="Trenk"

2010 VOL09 - a name used for backdoor trojan detections that have been added to Microsoft signatures after advanced automated analysis.

ms-caro-malware-full:malware-family="Tofsee"

2010 VOL09 - A multi-component family of backdoor trojans that act as a spam and traffic relay.

ms-caro-malware-full:malware-family="Ursap"

2010 VOL09 - a name used for backdoor trojan detections that have been added to Microsoft signatures after advanced automated analysis.

ms-caro-malware-full:malware-family="Zbot"

2010 VOL09 - A family of password stealing trojans that also contains backdoor functionality allowing unauthorized access and control of an affected machine.

ms-caro-malware-full:malware-family="Ciucio"

2010 VOL10 - A family of trojans that connect to certain websites in order to download arbitrary files.

ms-caro-malware-full:malware-family="ClickPotato"

2010 VOL10 - A program that displays popup and notification-style advertisements based on the user's browsing habits.

ms-caro-malware-full:malware-family="CVE-2010-0806"

2010 VOL10 - A detection for malicious JavaScript that attempts to exploit the vulnerability addressed by Microsoft Security Bulletin MS10-018.

ms-caro-malware-full:malware-family="Delf"

2010 VOL10 - A detection for various threats written in the Delphi programming language. The behaviors displayed by this malware family are highly variable.

ms-caro-malware-full:malware-family="FakePAV"

2010 VOL10 - A rogue security software family that masquerades as Microsoft Security Essentials.

ms-caro-malware-full:malware-family="Keygen"

2010 VOL10 - A generic detection for tools that generate product keys for illegally obtained versions of various software products.

ms-caro-malware-full:malware-family="Onescan"

2010 VOL10 - A Korean-language rogue security software family distributed under the names One Scan, Siren114, EnPrivacy, PC Trouble, My Vaccine, and others.

ms-caro-malware-full:malware-family="Pornpop"

2010 VOL10 - A generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.

ms-caro-malware-full:malware-family="Startpage"

2010 VOL10 - A detection for various threats that change the configured start page of the affected user's web browser, and may also perform other malicious actions.

ms-caro-malware-full:malware-family="Begseabug"

2011 VOL11 - A trojan that downloads and executes arbitrary files on an affected computer.

ms-caro-malware-full:malware-family="CVE-2010-0840"

2011 VOL11 - A detection for a malicious and obfuscated Java class that exploits a vulnerability described in CVE-2010-0840. Oracle Corporation addressed the vulnerability with a security update in March 2010.

ms-caro-malware-full:malware-family="Cycbot"

2011 VOL11 - A backdoor trojan that allows attackers unauthorized access and control of an affected computer. After a computer is infected, the trojan connects to a specific remote server to receive commands from attackers.

ms-caro-malware-full:malware-family="DroidDream"

2011 VOL11 - A malicious program that affects mobile devices running the Android operating system. It may be bundled with clean applications, and is capable of allowing a remote attacker to gain access to the mobile device.

ms-caro-malware-full:malware-family="FakeMacdef"

2011 VOL11 - A rogue security software family that affects Apple Mac OS X. It has been distributed under the names MacDefender, MacSecurity, MacProtector, and possibly others.

ms-caro-malware-full:malware-family="GameHack"

2011 VOL11 - Malware that is often bundled with game applications. It commonly displays unwanted pop-up advertisements and may be installed as a web browser helper object.

ms-caro-malware-full:malware-family="Loic"

2011 VOL11 - An open-source network attack tool designed to perform denial-ofservice (DoS) attacks.

ms-caro-malware-full:malware-family="Lotoor"

2011 VOL11 - A detection for specially crafted Android programs that attempt to exploit vulnerabilities in the Android operating system to gain root privilege.

ms-caro-malware-full:malware-family="Nuqel"

2011 VOL11 - A worm that spreads via mapped drives and certain instant messaging applications. It may modify system settings, connect to certain websites, download arbitrary files, or take other malicious actions.

ms-caro-malware-full:malware-family="OfferBox"

2011 VOL11 - A program that displays offers based on the user's web browsing habits. Some versions may display advertisements in a pop-under window. Win32/OfferBox may be installed without adequate user consent by malware.

ms-caro-malware-full:malware-family="OpenCandy"

2011 VOL11 - An adware program that may be bundled with certain thirdparty software installation programs. Some versions may send user-specific information, including a unique machine code, operating system information, locale, and certain other information to a remote server without obtaining adequate user consent.

ms-caro-malware-full:malware-family="Pameseg"

2011 VOL11 - A fake program installer that requires the user to send SMS messages to a premium number to successfully install certain programs.

ms-caro-malware-full:malware-family="Pramro"

2011 VOL11 - A trojan that creates a proxy on the infected computer for email and HTTP traffic, and is used to send spam email.

ms-caro-malware-full:malware-family="Ramnit"

2011 VOL11 - A family of multi-component malware that infects executable files, Microsoft Office files, and HTML files. Win32/Ramnit spreads to removable drives and steals sensitive information such as saved FTP credentials and browser cookies. It may also open a backdoor to await instructions from a remote attacker.

ms-caro-malware-full:malware-family="Rlsloup"

2011 VOL11 - A family of trojans that are used to send spam email. Rlsloup consists of several components, including an installation trojan component and a spamming payload component.

ms-caro-malware-full:malware-family="ShopperReports"

2011 VOL11 - Adware that displays targeted advertising to affected users while browsing the Internet, based on search terms entered into search engines.

ms-caro-malware-full:malware-family="Sinowal"

2011 VOL11 - A family of password-stealing and backdoor trojans. It may try to install a fraudulent SSL certificate on the computer. Sinowal may also capture user data such as banking credentials from various user accounts and send the data to Web sites specified by the attacker.

ms-caro-malware-full:malware-family="Stuxnet"

2011 VOL11 - A multi-component family that spreads via removable volumes by exploiting the

vulnerability addressed by Microsoft Security Bulletin MS10-046.

ms-caro-malware-full:malware-family="Swimnag"

2011 VOL11 - A worm that spreads via removable drives and drops a randomly-named DLL in the Windows system folder.

ms-caro-malware-full:malware-family="Tedroo"

2011 VOL11 - A trojan that sends spam email messages. Some variants may disable certain Windows services or allow backdoor access by a remote attacker.

ms-caro-malware-full:malware-family="Yimfoca"

2011 VOL11 - A worm family that spreads via common instant messaging applications and social networking sites. It is capable of connecting to a remote HTTP or IRC server to receive updated configuration data. It also modifies certain system and security settings.

ms-caro-malware-full:malware-family="Bamital"

2011 VOL12 - A family of malware that intercepts web browser traffic and prevents access to specific security-related websites by modifying the Hosts file. Bamital variants may also modify specific legitimate Windows files in order to execute their payload.

ms-caro-malware-full:malware-family="Blacole"

2011 VOL12 - An exploit pack, also known as Blackhole, that is installed on a compromised web server by an attacker and includes a number of exploits that target browser software. If a vulnerable computer browses a compromised website containing the exploit pack, various malware may be downloaded and run.

ms-caro-malware-full:malware-family="Bulilit"

2011 VOL12 - A trojan that silently downloads and installs other programs without consent. Infection could involve the installation of additional malware or malware components to an affected computer.

ms-caro-malware-full:malware-family="Dorkbot"

2011 VOL12 - A worm that spreads via instant messaging and removable drives. It also contains backdoor functionality that allows unauthorized access and control of the affected computer. Win32/Dorkbot may be distributed from compromised or malicious websites using PDF or browser exploits.

ms-caro-malware-full:malware-family="EyeStye"

2011 VOL12 - A trojan that attempts to steal sensitive data using a method known as form grabbing, and sends it to a remote attacker. It may also download and execute arbitary files and use a rootkit component to hide its activities.

ms-caro-malware-full:malware-family="FakeSysdef"

2011 VOL12 - A rogue security software family that claims to discover nonexistent hardware defects related to system memory, hard drives, and overall system performance, and charges a fee to fix the supposed problems.

ms-caro-malware-full:malware-family="Helompy"

2011 VOL12 - A worm that spreads via removable drives and attempts to capture and steal authentication details for a number of different websites or online services, including Facebook and Gmail.

ms-caro-malware-full:malware-family="Malf"

2011 VOL12 - A generic detection for malware that drops additional malicious files.

ms-caro-malware-full:malware-family="Rugo"

2011 VOL12 - A program that installs silently on the user's computer and displays advertisements.

ms-caro-malware-full:malware-family="Sirefef"

2011 VOL12 - A rogue security software family distributed under the name Antivirus 2010 and others.

ms-caro-malware-full:malware-family="Sisproc"

2011 VOL12 - A generic detection for a group of trojans that have been observed to perform a number of various and common malware behaviors.

ms-caro-malware-full:malware-family="Swisyn"

2011 VOL12 - A trojan that drops and executes arbitrary files on an infected computer. The dropped files may be potentially unwanted or malicious programs.

ms-caro-malware-full:malware-family="BlacoleRef"

2012 VOL13 - An obfuscated script, often found inserted into compromised websites, that uses a hidden inline frame to redirect the browser to a Blacole exploit server.

ms-caro-malware-full:malware-family="CVE-2012-0507"

2012 VOL13 - A detection for a malicious Java applet that exploits the Java Runtime Environment (JRE) vulnerability described in CVE-2012-0507, addressed by an Oracle security update in February 2012.

ms-caro-malware-full:malware-family="Flashback"

2012 VOL13 - A trojan that targets Java JRE vulnerability CVE-2012-0507 on Mac OS X to enroll the

infected computer in a botnet.

ms-caro-malware-full:malware-family="Gendows"

2012 VOL13 - A tool that attempts to activate Windows 7 and Windows Vista operating system installations.

ms-caro-malware-full:malware-family="GingerBreak"

2012 VOL13 - A program that affects mobile devices running the Android operating system. It drops and executes an exploit that, if run successfully, gains administrator privileges on the device.

ms-caro-malware-full:malware-family="GingerMaster"

2012 VOL13 - A malicious program that affects mobile devices running the Android operating system. It may be bundled with clean applications, and is capable of allowing a remote attacker to gain access to the mobile device.

ms-caro-malware-full:malware-family="Mult_JS"

2012 VOL13 - A generic detection for various exploits written in the JavaScript language.

ms-caro-malware-full:malware-family="Patch"

2012 VOL13 - A family of tools intended to modify, or 'patch' programs that may be evaluation copies, or unregistered versions with limited features for the purpose of removing the limitations.

ms-caro-malware-full:malware-family="Phoex"

2012 VOL13 - A malicious script that exploits the Java Runtime Environment (JRE) vulnerability discussed in CVE-2010-4452. If run in a computer running a vulnerable version of Java, it downloads and executes arbitrary files.

ms-caro-malware-full:malware-family="Pluzoks"

2012 VOL13 - A trojan that silently downloads and installs other programs without consent. This could include the installation of additional malware or malware components.

ms-caro-malware-full:malware-family="Popupper"

2012 VOL13 - A detection for a particular JavaScript script that attempts to display pop-under advertisements.

ms-caro-malware-full:malware-family="Wizpop"

2012 VOL13 - Adware that may track user search habits and download executable programs without user consent.

ms-caro-malware-full:malware-family="Wpakill"

2012 VOL13 - A family of tools that attempt to disable or bypass WPA (Windows Product Activation), WGA (Windows Genuine Advantage) checks, or WAT (Windows Activation Technologies), by altering Windows operating system files, terminating processes, or stopping services.

ms-caro-malware-full:malware-family="Yeltminky"

2012 VOL13 - A family of worms that spreads by making copies of itself on all available drives and creating an autorun.inf file to execute that copy.

ms-caro-malware-full:malware-family="Aimesu"

2013 VOL15 - A threat that exploits vulnerabilities in unpatched versions of Java, Adobe Reader, or Flash Player. It then installs other malare on the computer, including components of the Blackhole and Cool exploit kits.

ms-caro-malware-full:malware-family="Bdaejec"

2013 VOL15 - A trojan that allows unauthorized access and control of an affected computer, and that may download and install other programs without consent.

ms-caro-malware-full:malware-family="Bursted"

2013 VOL15 - A virus written in the AutoLISP scripting language used by the AutoCAD computer-aided design program. It infects other AutoLISP files with the extension .lsp.

ms-caro-malware-full:malware-family="Colkit"

2013 VOL15 - A detection for obfuscated, malicious JavaScript code that redirects to or loads files that may exploit a vulnerable version of Java, Adobe Reader, or Adobe Flash, possibly in an attempt to load malware onto the computer.

ms-caro-malware-full:malware-family="Coolex"

2013 VOL15 - A detection for scripts from an exploit pack known as the Cool Exploit Kit. These scripts are often used in ransomware schemes in which an attacker locks a victim’s computer or encrypts the user’s data and demands money to make it available again.

ms-caro-malware-full:malware-family="CplLnk"

2013 VOL15 - A generic detection for specially crafted malicious shortcut files that attempt to exploit the vulnerability addressed by Microsoft Security Bulletin MS10-046, CVE-2010-2568.

ms-caro-malware-full:malware-family="CVE-2011-1823"

2013 VOL15 - A detection for specially crafted Android programs that attempt to exploit a vulnerability in the Android operating system to gain root privilege.

ms-caro-malware-full:malware-family="CVE-2012-1723"

2013 VOL15 - A family of malicious Java applets that attempt to exploit vulnerability CVE-2012-1723 in the Java Runtime Environment (JRE) to download and install files of an attacker’s choice onto the computer.

ms-caro-malware-full:malware-family="DealPly"

2013 VOL15 - Adware that displays offers related to the user’s web browsing habits. It may be bundled with certain third-party software installation programs.

ms-caro-malware-full:malware-family="Fareit"

2013 VOL15 - A malware family that has multiple components: a password stealing component that steals sensitive information and sends it to an attacker, and a DDoS component that could be used against other computers.

ms-caro-malware-full:malware-family="FastSaveApp"

2013 VOL15 - An adware program that displays offers related to the user’s web browsing habits. It may use the name 'SaveAs' or 'SaveByClick'.

ms-caro-malware-full:malware-family="FindLyrics"

2013 VOL15 - An adware program that displays ads related to the user’s web browsing habits.

ms-caro-malware-full:malware-family="Gamarue"

2013 VOL15 - A worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.

ms-caro-malware-full:malware-family="Gisav"

2013 VOL15 - An adware program that displays offers related to the user’s web browsing habits. It can be downloaded from the program’s website, and can be bundled with some third-party software installation programs.

ms-caro-malware-full:malware-family="InfoAtoms"

2013 VOL15 - An adware program that displays advertisements related to the user’s web browsing habits and inserts advertisements into websites.

ms-caro-malware-full:malware-family="Perl/IRCbot.E"

2013 VOL15 - A backdoor trojan that drops other malicious software and connects to IRC servers to receive commands from attackers.

ms-caro-malware-full:malware-family="Javrobat"

2013 VOL15 - An exploit that tries to check whether certain versions of Adobe Acrobat or Adobe Reader are installed on the computer. If so, it tries to install malware.

ms-caro-malware-full:malware-family="Kraddare"

2013 VOL15 - Adware that displays Korean-language advertisements.

ms-caro-malware-full:malware-family="PriceGong"

2013 VOL15 - An adware program that shows certain deals related to the search terms entered on any web page.

ms-caro-malware-full:malware-family="Protlerdob"

2013 VOL15 - A software installer with a Portuguese language user interface. It presents itself as a free movie download but bundles with it a number of programs that may charge for services.

ms-caro-malware-full:malware-family="Qhost"

2013 VOL15 - A generic detection for trojans that modify the HOSTS file on the computer to redirect or limit Internet traffic to certain sites.

ms-caro-malware-full:malware-family="Reveton"

2013 VOL15 - A ransomware family that targets users from certain countries or regions. It locks the computer and displays a location-specific webpage that covers the desktop and demands that the user pay a fine for the supposed possession of illicit material.

ms-caro-malware-full:malware-family="Rongvhin"

2013 VOL15 - A family of malware that perpetrates click fraud. It might be delivered to the computer via hack tools for the game CrossFire.

ms-caro-malware-full:malware-family="Seedabutor"

2013 VOL15 - A JavaScript trojan that attempts to redirect the browser to another website.

ms-caro-malware-full:malware-family="SMSer"

2013 VOL15 - A ransomware trojan that locks an affected user’s computer and requests that the user send a text message to a premium-charge number to unlock it.

ms-caro-malware-full:malware-family="Tobfy"

2013 VOL15 - A family of ransomware trojans that targets users from certain countries. It locks the computer and displays a localized message demanding the payment of a fine for the supposed possession of illicit material. Some variants may also take webcam screenshots, play audio

messages, or affect certain processes or drivers.

ms-caro-malware-full:malware-family="Truado"

2013 VOL15 - A trojan that poses as an update for certain Adobe software.

ms-caro-malware-full:malware-family="Urausy"

2013 VOL15 - A family of ransomware trojans that locks the computer and displays a localized message, supposedly from police authorities, demanding the payment of a fine for alleged criminal activity.

ms-caro-malware-full:malware-family="Wecykler"

2013 VOL15 - A family of worms that spread via removable drives, such as USB drives, that may stop security processes and other processes on the computer, and log keystrokes that are later sent to a remote attacker.

ms-caro-malware-full:malware-family="Weelsof"

2013 VOL15 - A family of ransomware trojans that targets users from certain countries. It locks the computer and displays a localized message demanding the payment of a fine for the alleged possession of illicit material. Some variants may take steps that make it difficult to run or update virus protection.

ms-caro-malware-full:malware-family="Yakdowpe"

2013 VOL15 - A family of trojans that connect to certain websites to silently download and install other programs without consent.

ms-caro-malware-full:malware-family="Anogre"

2013 VOL16 - A threat that exploits a vulnerability addressed by Microsoft Security Bulletin MS11-087. This vulnerability can allow a hacker to install programs, view, change, or delete data or create new accounts with full administrative privileges.

ms-caro-malware-full:malware-family="Brantall"

2013 VOL16 - A family of trojans that download and install other programs, including Win32/Sefnit and Win32/Rotbrow. Brantall often pretends to be an installer for other, legitimate programs.

ms-caro-malware-full:malware-family="Comame"

2013 VOL16 - A generic detection for a variety of threats.

ms-caro-malware-full:malware-family="Crilock"

2013 VOL16 - A ransomware family that encrypts the computer’s files and displays a webpage that demands a fee to unlock them.

ms-caro-malware-full:malware-family="CVE-2011-3874"

2013 VOL16 - A threat that attempts to exploit a vulnerability in the Android operating system to gain access to and control of the device Java/CVE-2012-1723. A family of malicious Java applets that attempt to exploit vulnerability CVE-2012-1723 in the Java Runtime Environment (JRE) in order to download and install files of an attacker's choice onto the computer.

ms-caro-malware-full:malware-family="Deminnix"

2013 VOL16 - A trojan that uses the computer for Bitcoin mining and changes the home page of the web browser. It can accidentally be downloaded along with other files from torrent sites.

ms-caro-malware-full:malware-family="Detplock"

2013 VOL16 - A generic detection for a variety of threats.

ms-caro-malware-full:malware-family="Dircrypt"

2013 VOL16 - Ransomware that encrypts the user's files and demands payment to release them. It is distributed through spam email messages and can be downloaded by other malware.

ms-caro-malware-full:malware-family="DonxRef"

2013 VOL16 - A generic detection for malicious JavaScript objects that construct shellcode. The scripts may try to exploit vulnerabilities in Java, Adobe Flash Player, and Windows.

ms-caro-malware-full:malware-family="Faceliker"

2013 VOL16 - A malicious script that likes content on Facebook without the user's knowledge or consent.

ms-caro-malware-full:malware-family="FakeAlert"

2013 VOL16 - A malicious script that falsely claims that the computer is infected with viruses and that additional software is needed to disinfect it.

ms-caro-malware-full:malware-family="Jenxcus"

2013 VOL16 - A worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.

ms-caro-malware-full:malware-family="Loktrom"

2013 VOL16 - Ransomware that locks the computer and displays a full-screen message pretending to be from a national police force, demanding payment to unlock the computer.

ms-caro-malware-full:malware-family="Miposa"

2013 VOL16 - A trojan that downloads and runs malicious Windows Scripting Host (.wsh) files.

ms-caro-malware-full:malware-family="Nitol"

2013 VOL16 - A family of trojans that perform DDoS (distributed denial of service) attacks, allow backdoor access and control, download and run files, and perform a number of other malicious activities on the computer.

ms-caro-malware-full:malware-family="Oceanmug"

2013 VOL16 - A trojan that silently downloads and installs other programs without consent.

ms-caro-malware-full:malware-family="Proslikefan"

2013 VOL16 - A worm that spreads through removable drives, network shares, and P2P programs. It can lower the computer's security settings and disable antivirus products.

ms-caro-malware-full:malware-family="Rotbrow"

2013 VOL16 - A trojan that installs browser add-ons that claim to offer protection from other add-ons. Rotbrow can change the browser's home page, and can install the trojan Win32/Sefnit. It is commonly installed by Win32/Brantall.

ms-caro-malware-full:malware-family="Sefnit"

2013 VOL16 - A family of trojans that can allow backdoor access, download files, and use the computer and Internet connection for click fraud. Some variants can monitor web browsers and hijack search results.

ms-caro-malware-full:malware-family="Urntone"

2013 VOL16 - A webpage component of the Neutrino exploit kit. It checks the version numbers of popular applications installed on the computer, and attempts to install malware that targets vulnerabilities in the software.

ms-caro-malware-full:malware-family="Wysotot"

2013 VOL16 - A threat that can change the start page of the user's web browser, and may download and install other files to the computer. It is installed by software bundlers that advertise free software or games.

ms-caro-malware-full:malware-family="AddLyrics"

2014 VOL17 - A browser add-on that displays lyrics for songs on YouTube, and displays advertisements in the browser window.

ms-caro-malware-full:malware-family="Adpeak"

2014 VOL17 - Adware that displays extra ads as the user browses the Internet, without revealing where the ads are coming from. It may be bundled with some third-party software installation programs.

ms-caro-malware-full:malware-family="Axpergle"

2014 VOL17 - A detection for the Angler exploit kit, which exploits vulnerabilities in recent versions of Internet Explorer, Silverlight, Adobe Flash Player, and Java to install malware.

ms-caro-malware-full:malware-family="Bepush"

2014 VOL17 - A family of trojans that download and install add-ons for the Firefox and Chrome browsers that post malicious links to social networking sites, track browser usage, and redirect the browser to specific websites.

ms-caro-malware-full:malware-family="BetterSurf"

2014 VOL17 - Adware that displays unwanted ads on search engine results pages and other websites. It may be included with software bundles that offer free applications or games.

ms-caro-malware-full:malware-family="Bladabindi"

2014 VOL17 - A family of backdoors created by a malicious hacker tool called NJ Rat. They can steal sensitive information, download other malware, and allow backdoor access to an infected computer.

ms-caro-malware-full:malware-family="Caphaw"

2014 VOL17 - A family of backdoors that spread via Facebook, YouTube, Skype, removable drives, and drive-by download. They can make Facebook posts via the user’s account, and may steal online banking details.

ms-caro-malware-full:malware-family="Clikug"

2014 VOL17 - A threat that uses a computer for click fraud. It has been observed using as much as a gigabyte of bandwidth per hour.

ms-caro-malware-full:malware-family="CVE-2014-0322"

This threat uses a vulnerability MS14-012, CVE-2014-0322 in Internet Explorer 9 and 10 to download and run files on your PC, including other malware.

ms-caro-malware-full:malware-family="CVE-2013-0422"

2014 VOL17 - A detection for a malicious Java applet that exploits the Java Runtime Environment (JRE) vulnerability described in CVE-2013-0422, addressed by an Oracle security update in January 2013.

ms-caro-malware-full:malware-family="Dowque"

2014 VOL17 - A generic detection for malicious files that are capable of installing other malware.

ms-caro-malware-full:malware-family="Fashack"

2014 VOL17 - A detection for the Safehack exploit kit, also known as Flashpack. It uses vulnerabilities in Adobe Flash Player, Java, and Silverlight to install malware on a computer.

ms-caro-malware-full:malware-family="Feven"

2014 VOL17 - A browser add-on for Internet Explorer, Firefox, or Chrome that displays ads on search engine results pages and other websites, and redirects the browser to specific websites.

ms-caro-malware-full:malware-family="Fiexp"

2014 VOL17 - A detection for the Fiesta exploit kit, which attempts to exploit Java, Adobe Flash Player, Adobe Reader, Silverlight, and Internet Explorer to install malware.

ms-caro-malware-full:malware-family="Filcout"

2014 VOL17 - An application that offers to locate and download programs to run unknown files. It has been observed installing variants in the Win32/Sefnit family.

ms-caro-malware-full:malware-family="Genasom"

2014 VOL17 - A ransomware family that locks a computer and demands money to unlock it. It usually targets Russian-language users, and may open pornographic websites.

ms-caro-malware-full:malware-family="Kegotip"

2014 VOL17 - A password-stealing trojan that can steal email addresses, personal information, or user account information for certain programs.

ms-caro-malware-full:malware-family="Krypterade"

2014 VOL17 - Ransomware that fraudulently claims a computer has been used for unlawful activity, locks it, and demands that the user pay to unlock it.

ms-caro-malware-full:malware-family="Lecpetex"

2014 VOL17 - A family of trojans that steal sensitive information, such as user names and passwords. It can also use a computer for Litecoin mining, install other malware, and post malicious content via the user’s Facebook account.

ms-caro-malware-full:malware-family="Lollipop"

2014 VOL17 - Adware that may be installed by third-party software bundlers. It displays ads based on search engine searches, which can differ by geographic location and may be pornographic.

ms-caro-malware-full:malware-family="Meadgive"

2014 VOL17 - A detection for the Redkit exploit kit, also known as Infinity and Goon. It attempts to

exploit vulnerabilities in programs such as Java and Silverlight to install other malware.

ms-caro-malware-full:malware-family="Neclu"

2014 VOL17 - A detection for the Nuclear exploit kit, which attempts to exploit vulnerabilities in programs such as Java and Adobe Reader to install other malware.

ms-caro-malware-full:malware-family="Ogimant"

2014 VOL17 - A threat that claims to help download items from the Internet, but actually downloads and runs files that are specified by a remote attacker.

ms-caro-malware-full:malware-family="OptimizerElite"

2014 VOL17 - A misleading program that uses legitimate files in the Prefetch folder to claim that the computer is damaged, and offers to fix the damage for a price.

ms-caro-malware-full:malware-family="Pangimop"

2014 VOL17 - A detection for the Magnitude exploit kit, also known as Popads. It attempts to exploit vulnerabilities in programs such as Java and Adobe Flash Player to install other malware.

ms-caro-malware-full:malware-family="Phish"

2014 VOL17 - A password-stealing malicious webpage, known as a phishing page, that disguises itself as a page from a legitimate website.

ms-caro-malware-full:malware-family="Prast"

2014 VOL17 - A generic detection for various password stealing trojans.

ms-caro-malware-full:malware-family="Slugin"

2014 VOL17 - A file infector that infects .exe and .dll files. It may also perform backdoor actions.

ms-caro-malware-full:malware-family="Spacekito"

2014 VOL17 - A threat that steals information about the computer and installs browser add-ons that display ads.

ms-caro-malware-full:malware-family="Tranikpik"

This threat is a backdoor that can give a hacker unauthorized access and control of your PC

ms-caro-malware-full:malware-family="Wordinvop"

2014 VOL17 - A detection for a specially-crafted Microsoft Word file that attempts to exploit the vulnerability CVE-2006-6456, addressed by Microsoft Security Bulletin MS07-014.

ms-caro-malware-full:malware-family="Zegost"

2014 VOL17 - A backdoor that allows an attacker to remotely access and control a computer.

ms-caro-malware-full:malware-family="Archost"

2014 VOL18 - A downloader that installs other programs on the computer without the user's consent, including other malware.

ms-caro-malware-full:malware-family="Balamid"

2014 VOL18 - A trojan that can use the computer to click on online advertisements without the user's permission or knowledge. This can earn money for a malicious hacker by making a website or application appear more popular than it is.

ms-caro-malware-full:malware-family="BeeVry"

2014 VOL18 - A trojan that modifies a number of settings to prevent the computer from accessing security-related websites, and lower the computer's security.

ms-caro-malware-full:malware-family="Bondat"

2014 VOL18 - A family of threats that collects information about the computer, infects removable drives, and tries to stop the user from accessing files. It spreads by infecting removable drives, such as USB thumb drives and flash drives.

ms-caro-malware-full:malware-family="Bregent"

2014 VOL18 - A downloader that injects malicious code into legitimate processes such as explorer.exe and svchost.exe, and downloads other malware onto the computer.

ms-caro-malware-full:malware-family="Brolo"

2014 VOL18 - A ransomware family that locks the web browser and displays a message, often pretending to be from a law enforcement agency, demanding money to unlock the browser.

ms-caro-malware-full:malware-family="CostMin"

2014 VOL18 - An adware family that installs itself as a browser extension for Internet Explorer, Mozilla Firefox, and Google Chrome, and displays advertisements as the user browses the Internet.

ms-caro-malware-full:malware-family="CouponRuc"

2014 VOL18 - A browser modifier that changes browser settings and may also modify some computer and Internet settings.

ms-caro-malware-full:malware-family="Crastic"

2014 VOL18 - A trojan that sends sensitive information to a remote attacker, such as user names,

passwords and information about the computer. It can also delete System Restore points, making it harder to recover the computer to a pre-infected state.

ms-caro-malware-full:malware-family="Crowti"

2014 VOL18 - A ransomware family that encrypts files on the computer and demands that the user pay a fee to decrypt them, using Bitcoins.

ms-caro-malware-full:malware-family="CVE-2013-1488"

2014 VOL18 - A detection for threats that use a Java vulnerability to download and run files on your PC, including other malware. Oracle addressed the vulnerability with a security update in April 2013.

ms-caro-malware-full:malware-family="DefaultTab"

2014 VOL18 - A browser modifier that redirects web browser searches and prevents the user from changing browser settings.

ms-caro-malware-full:malware-family="Ippedo"

2014 VOL18 - A worm that can send sensitive information to a malicious hacker. It spreads through infected removable drives, such as USB flash drives.

ms-caro-malware-full:malware-family="Kilim"

2014 VOL18 - A trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.

ms-caro-malware-full:malware-family="Mofin"

2014 VOL18 - A worm that can steal files from your PC and send them to a malicious hacker. It spreads via infected removable drives, such as USB flash drives.

ms-caro-malware-full:malware-family="MpTamperSrp"

2014 VOL18 - A generic detection for an attempt to add software restriction policies to restrict Microsoft antimalware products, such as Microsoft Security Essentials and Windows Defender, from functioning properly.

ms-caro-malware-full:malware-family="Mujormel"

2014 VOL18 - A password stealer that can steal personal information, such as user names and passwords, and send the stolen information to a malicious hacker.

ms-caro-malware-full:malware-family="PennyBee"

2014 VOL18 - Adware that shows ads as the user browses the web. It can be installed from the

program's website or bundled with some third-party software installation programs.

ms-caro-malware-full:malware-family="Phdet"

2014 VOL18 - A family of backdoor trojans that is used to perform distributed denial-of service (DDoS) attacks against specified targets.

ms-caro-malware-full:malware-family="Rimod"

2014 VOL18 - A generic detection for files that change various security settings in the computer Win32/Rotbrow. A trojan that installs browser add-ons that claim to offer protection from other add-ons. Rotbrow can change the browser's home page, and can install the trojan Win32/Sefnit. It is commonly installed by Win32/Brantall.

ms-caro-malware-full:malware-family="Sigru"

2014 VOL18 - A virus that can stop some files from working correctly in Windows XP and earlier operating systems. It spreads by infecting the master boot record (MBR) on connected hard disks and floppy disks.

ms-caro-malware-full:malware-family="SimpleShell"

2014 VOL18 - A backdoor that can give a malicious hacker unauthorized access to and control of the computer.

ms-caro-malware-full:malware-family="Softpulse"

2014 VOL18 - A software bundler that no longer meets Microsoft detection criteria for unwanted software following a program update in September of 2014.

ms-caro-malware-full:malware-family="SquareNet"

2014 VOL18 - A software bundler that installs other unwanted software, including adware and click-fraud malware.

ms-caro-malware-full:malware-family="Tugspay"

2014 VOL18 - A downloader that spreads by posing as an installer for legitimate software, such as a Java update, or through other malware. When installed, it downloads unwanted software to the computer.

ms-caro-malware-full:malware-family="Tupym"

2014 VOL18 - A worm that copies itself to the system folder of the affected computer, and attempts to contact remote hosts.

ms-caro-malware-full:malware-family="Vercuser"

2014 VOL18 - A worm that typically spreads via drive-by download. It also receives commands from

a remote server, and has been observed dropping other malware on the infected computer.

ms-caro-malware-full:malware-family="Adnel"

2015 VOL19 - A family of macro malware that can download other threats to the computer, including TrojanDownloader:Win32/Drixed.

ms-caro-malware-full:malware-family="Adodb"

2015 VOL19 - A generic detection for script trojans that exploit a vulnerability in Microsoft Data Access Components (MDAC) that allows remote code execution. Microsoft released Security Bulletin MS06-014 in April 2006 to address the vulnerability.

ms-caro-malware-full:malware-family="AlterbookSP"

2015 VOL19 - A browser add-on that formerly displayed behaviors of unwanted software. Recent versions of the add-on no longer meet Microsoft detection criteria, and are no longer considered unwanted software.

ms-caro-malware-full:malware-family="BrobanDel"

2015 VOL19 - A family of trojans that can modify boletos bancários, a common payment method in Brazil. They can be installed on the computer when a user opens a malicious spam email attachment.

ms-caro-malware-full:malware-family="CompromisedCert"

2015 VOL19 - A detection for the Superfish VisualDiscovery advertising program that was preinstalled on some Lenovo laptops sold in 2014 and 2015. It installs a compromised trusted root certificate on the computer, which can be used to conduct man-in-the-middle attacks on the computer.

ms-caro-malware-full:malware-family="CouponRuc_new"

2015 VOL19 - A browser modifier that changes browser settings and may also modify some computer and Internet settings.

ms-caro-malware-full:malware-family="CVE-2014-6332"

2015 VOL19 - This threat uses a Microsoft vulnerability MS14-064 to download and run files on your PC, including other malware.

ms-caro-malware-full:malware-family="Dyzap"

2015 VOL19 - A threat that steals login credentials for a long list of banking websites using man-in-the-browser (MITB) attacks. It is usually installed on the infected computer by TrojanDownloader:Win32/Upatre.

ms-caro-malware-full:malware-family="EoRezo"

2015 VOL19 - Adware that displays targeted advertising to affected users while browsing the Internet, based on downloaded pre-configured information.

ms-caro-malware-full:malware-family="FakeCall"

2015 VOL19 - This threat is a webpage that claims your PC is infected with malware. It asks you to phone a number to receive technical support to help remove the malware.

ms-caro-malware-full:malware-family="Foosace"

2015 VOL19 - A threat that creates files on the compromised computer and contacts a remote host. Observed in the STRONTIUM APT.

ms-caro-malware-full:malware-family="IeEnablerCby"

2015 VOL19 - A browser modifier that installs additional browser addons without the user’s consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.

ms-caro-malware-full:malware-family="InstalleRex"

2015 VOL19 - A software bundler that installs unwanted software, including Win32/CouponRuc and Win32/SaverExtension. It alters its own 'Installed On' date in Programs and Features to make it more difficult for a user to locate it and remove it.

ms-caro-malware-full:malware-family="JackTheRipper"

2015 VOL19 - A virus that can stop some files from working correctly in Windows XP and earlier operating systems. It spreads by infecting the master boot record (MBR) on connected hard disks and floppy disks.

ms-caro-malware-full:malware-family="Kenilfe"

2015 VOL19 - A worm written in AutoCAD Lisp that only runs if AutoCAD is installed on the computer or network. It renames and deletes certain AutoCAD files, and may download and execute arbitrary files from a remote host.

ms-caro-malware-full:malware-family="KipodToolsCby"

2015 VOL19 - A browser modifier that installs additional browser addons without the user’s consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.

ms-caro-malware-full:malware-family="Macoute"

2015 VOL19 - A worm that can spread itself to removable USB drives, and may communicate with a remote host.

ms-caro-malware-full:malware-family="NeutrinoEK"

2015 VOL19 - This threat is a webpage that spreads the exploit kit known as Neutrino.

ms-caro-malware-full:malware-family="Peaac"

2015 VOL19 - A generic detection for various threats that display trojan characteristics.

ms-caro-malware-full:malware-family="Peals"

2015 VOL19 - A generic detection for various threats that display trojan characteristics.

ms-caro-malware-full:malware-family="Radonskra"

2015 VOL19 - A family of threats that perform a variety of malicious acts, including stealing information about the computer, showing extra advertisements as the user browses the web, performing click fraud, and downloading other programs without consent.

ms-caro-malware-full:malware-family="SaverExtension"

2015 VOL19 - A browser add-on that shows ads in the browser without revealing their source, and prevents itself from being removed normally.

ms-caro-malware-full:malware-family="Sdbby"

2015 VOL19 - A threat that exploits a bypass to gain administrative privileges on a machine without going through a User Access Control prompt.

ms-caro-malware-full:malware-family="Simda"

2015 VOL19 - A threat that can give an attacker backdoor access and control of an infected computer. It can then steal passwords and gather information about the computer to send to the attacker.

ms-caro-malware-full:malware-family="Skeeyah"

2015 VOL19 - A generic detection for various threats that display trojan characteristics.

ms-caro-malware-full:malware-family="Wordjmp"

2015 VOL19 - An exploit that targets a vulnerability in Word 2002 and 2003 that could allow an attacker to remotely execute arbitrary code. Microsoft released Security Bulletin MS06-027 in June 2006 to address the vulnerability.

ms-caro-malware-full:malware-family="Bayads"

2015 VOL20 - A program that displays ads as the user browses the web. It can be bundled with other software. It may call itself bdraw, delta, dlclient, Pay-ByAds, or pricehorse in Programs and Features.

ms-caro-malware-full:malware-family="CandyOpen"

2015 VOL20 - This application can also affect the quality of your computing experience. We have seen this leading to the following potentially unwanted behaviors on PCs: Adds files that run at startup, Modifies boot configuration data, Modifies file associations, Injects into other processes on your system, Changes browser settings, Adds a local proxy, Modifies your system DNS settings, Stops Windows Update, Disables User Access Control (UAC), These applications are most commonly software bundlers or installers for applications such as toolbars, adware, or system optimizers. We have observed this application installing software that you might not have intended on your PC.

ms-caro-malware-full:malware-family="Colisi"

2015 VOL20 - Behavioral detection of certain files acting in a malicious way.

ms-caro-malware-full:malware-family="Creprote"

2015 VOL20 - These programs are most commonly software bundlers or installers for software such as toolbars, adware, or system optimizers. The software might modify your homepage, your search provider, or perform other actions that you might not have intended.

ms-caro-malware-full:malware-family="Diplugem"

2015 VOL20 - A browser modifier that installs browser add-ons without obtaining the user’s consent. The add-ons show extra advertisements as the user browses the web, and can inject additional ads into web search results pages.

ms-caro-malware-full:malware-family="Dipsind"

2015 VOL20 - A threat that is often used in targeted attacks. It can give an attacker access to the computer to download and run files, steal domain credentials, and perform other malicious actions.

ms-caro-malware-full:malware-family="Donoff"

2015 VOL20 - A threat that uses an infected Microsoft Office file to download other malware onto the computer. It can arrive as a spam email attachment, usually as a Word file (.doc).

ms-caro-malware-full:malware-family="Dorv"

2015 VOL20 - A trojan is a type of malware that can’t spread on its own. It relies on you to run them on your PC by mistake, or visit a hacked or malicious webpage. They can steal your personal information, download more malware, or give a malicious hacker access to your PC.

ms-caro-malware-full:malware-family="Dowadmin"

2015 VOL20 - A software bundler that does not provide the user with the option to decline installation of unwanted software.

ms-caro-malware-full:malware-family="Fourthrem"

2015 VOL20 - A program that installs unwanted software without adequate consent on the computer at the same time as the software the user is trying to install.

ms-caro-malware-full:malware-family="Hao123"

2015 VOL20 - This threat is a modified Internet Explorer shortcut that changes your Internet Explorer homepage. It might arrive on your PC through bundlers that offer free software. The threat will run a separate threat-related file that changes the Internet Explorer.

ms-caro-malware-full:malware-family="Mizenota"

2015 VOL20 - This program is a software bundler that installs unwanted software on your PC at the same time as the software you are trying to install. It may install one of the following: BrowserModifier:Win32/SupTab, BrowserModifier:Win32/Sasquor, BrowserModifier:Win32/Smudplu, SoftwareBundler:Win32/Pokavampo, BrowserModifier:Win32/Shopperz, Adware:Win32/EoRezo

ms-caro-malware-full:malware-family="Mytonel"

2015 VOL20 - A program that downloads and installs other programs onto the computer without the user’s consent, including other malware.

ms-caro-malware-full:malware-family="OutBrowse"

2015 VOL20 - A software bundler that installs additional unwanted programs alongside software that the user wishes to install. It can remove or hide the installer’s close button, leaving no way to decline the additional applications.

ms-caro-malware-full:malware-family="Peapoon"

2015 VOL20 - An adware program that shows users ads that they cannot control as they browse the web. It may identify itself as Coupon in Programs and Features.

ms-caro-malware-full:malware-family="Pokki"

2015 VOL20 - A browser add-on that formerly displayed behaviors of unwanted software. Recent versions of the add-on no longer meet Microsoft detection criteria, and are no longer considered unwanted software.

ms-caro-malware-full:malware-family="Putalol"

2015 VOL20 - An adware program that shows users ads that they cannot control as they browse the web. It may identify itself as Lolliscan in Programs and Features.

ms-caro-malware-full:malware-family="SpigotSearch"

2015 VOL20 - This application can affect the quality of your computing experience. For example,

some potentially unwanted applications can: Install additional bundled software, Modify your homepage, Modify your search provider. These applications are most commonly software bundlers or installers for applications such as toolbars, adware, or system optimizers. We have observed this application installing software that you might not have intended on your PC.

ms-caro-malware-full:malware-family="Spursint"

2015 VOL20 - This threat has been detected as one of the executable malware that are distributed through URLs.

ms-caro-malware-full:malware-family="Sulunch"

2015 VOL20 - A generic detection for a group of trojans that perform a number of common malware behaviors.

ms-caro-malware-full:malware-family="SupTab"

2015 VOL20 - A browser modifier that installs itself and changes the browser's default search provider, without obtaining the user's consent for either action.

ms-caro-malware-full:malware-family="Sventore"

2015 VOL20 - This trojan can install other malware or unwanted software onto your PC.

ms-caro-malware-full:malware-family="Tillail"

2015 VOL20 - A software bundler that installs unwanted software alongside the software the user is trying to install. It has been observed to install the browser modifier Win32/SupTab.

ms-caro-malware-full:malware-family="VOPackage"

2015 VOL20 - This application can also affect the quality of your computing experience. We have seen this leading to the following potentially unwanted behaviors on PCs: Adds files that run at startup, Installs a driver, Injects into other processes on your system, Injects into browsers, Changes browser settings, Changes browser shortcuts, Installs browser extensions, Adds a local proxy, Tampers with root certificate trust, Modifies the system hosts file, Modifies your system DNS settings, Disables anti-virus products, Tampers with system Group Policy settings, These applications are most commonly software bundlers or installers for applications such as toolbars, adware, or system optimizers. We have observed this application installing software that you might not have intended on your PC.

ms-caro-malware-full:malware-family="Xiazai"

2015 VOL20 - A program that installs unwanted software on the computer at the same time as the software the user is trying to install, without adequate consent.

nato

nato namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

NATO classification markings.

classification

nato:classification="CTS"

COSMIC TOP SECRET

nato:classification="CTS-B"

COSMIC TOP SECRET BOHEMIA

nato:classification="NS"

NATO SECRET

nato:classification="NC"

NATO CONFIDENTIAL

nato:classification="NR"

NATO RESTRICTED

nato:classification="NU"

NATO UNCLASSIFIED

nato:classification="CTS-A"

COSMIC TOP SECRET ATOMAL

nato:classification="NS-A"

SECRET ATOMAL

nato:classification="NC-A"

CONFIDENTIAL ATOMAL

open_threat

open_threat namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Open Threat Taxonomy v1.1 base on James Tarala of SANS http://www.auditscripts.com/resources/open_threat_taxonomy_v1.1a.pdf, https://files.sans.org/summit/Threat_Hunting_Incident_Response_Summit_2016/PDFs/Using-Open-Tools-to-Convert-Threat-Intelligence-into-Practical-Defenses-James-Tarala-SANS-Institute.pdf, https://www.youtube.com/watch?v=5rdGOOFC_yE, and https://www.rsaconference.com/writable/presentations/file_upload/str-r04_using-an-open-source-threat-model-for-prioritized-defense-final.pdf

threat-category

open_threat:threat-category="Physical"

Threats to the confidentiality, integrity, or availability of information systems that are physical in nature. These threats generally describe actions that could lead to the theft, harm, or destruction of information systems.

open_threat:threat-category="Resource"

Threats to the confidentiality, integrity, or availability of information systems that are the result of a lack of resources required by the information system. These threats often cause failures of information systems through a disruption of resources required for operations.

open_threat:threat-category="Personal"

Threats to the confidentiality, integrity, or availability of information systems that are the result of failures or actions performed by an organization's personnel. These threats can be the result of deliberate or accidental actions that cause harm to information systems.

open_threat:threat-category="Technical"

Threats to the confidentiality, integrity, or availability of information systems that are technical in nature. These threats are most often considered when identifying threats and constitute the technical actions performed by a threat actor that can cause harm to an information system.

threat-name

open_threat:threat-name="PHY-001"

Loss of Property - Rating: 5.0

open_threat:threat-name="PHY-002"

Theft of Property - Rating: 5.0

open_threat:threat-name="PHY-003"

Accidental Destruction of Property - Rating: 3.0

open_threat:threat-name="PHY-004"

Natural Destruction of Property - Rating: 3.0

open_threat:threat-name="PHY-005"

Intentional Destruction of Property - Rating: 2.0

open_threat:threat-name="PHY-006"

Intentional Sabotage of Property - Rating: 2.0

open_threat:threat-name="PHY-007"

Intentional Vandalism of Property - Rating: 2.0

open_threat:threat-name="PHY-008"

Electrical System Failure - Rating: 4.0

open_threat:threat-name="PHY-009"

Heating, Ventilation, Air Conditioning (HVAC) Failure - Rating: 3.0

open_threat:threat-name="PHY-010"

Structural Facility Failure - Rating: 2.0

open_threat:threat-name="PHY-011"

Water Distribution System Failure - Rating: 2.0

open_threat:threat-name="PHY-012"

Sanitation System Failure - Rating: 1.0

open_threat:threat-name="PHY-013"

Natural Gas Distribution Failure - Rating: 1.0

open_threat:threat-name="PHY-014"

Electronic Media Failure - Rating: 3.0

open_threat:threat-name="RES-001"

Disruption of Water Resources - Rating: 2.0

open_threat:threat-name="RES-002"

Disruption of Fuel Resources - Rating: 2.0

open_threat:threat-name="RES-003"

Disruption of Materials Resources - Rating: 2.0

open_threat:threat-name="RES-004"

Disruption of Electrical Resources - Rating: 4.0

open_threat:threat-name="RES-005"

Disruption of Transportation Services - Rating: 1.0

open_threat:threat-name="RES-006"

Disruption of Communications Services - Rating: 4.0

open_threat:threat-name="RES-007"

Disruption of Emergency Services - Rating: 1.0

open_threat:threat-name="RES-008"

Disruption of Governmental Services - Rating: 1.0

open_threat:threat-name="RES-009"

Supplier Viability - Rating: 2.0

open_threat:threat-name="RES-010"

Supplier Supply Chain Failure - Rating: 2.0

open_threat:threat-name="RES-011"

Logistics Provider Failures - Rating: 1.0

open_threat:threat-name="RES-012"

Logistics Route Disruptions - Rating: 1.0

open_threat:threat-name="RES-013"

Technology Services Manipulation - Rating: 3.0

open_threat:threat-name="PER-001"

Personnel Labor / Skills Shortage - Rating: 5.0

open_threat:threat-name="PER-002"

Loss of Personnel Resources - Rating: 3.0

open_threat:threat-name="PER-003"

Disruption of Personnel Resources - Rating: 3.0

open_threat:threat-name="PER-004"

Social Engineering of Personnel Resources - Rating: 4.0

open_threat:threat-name="PER-005"

Negligent Personnel Resources - Rating: 4.0

open_threat:threat-name="PER-006"

Personnel Mistakes / Errors - Rating: 4.0

open_threat:threat-name="PER-007"

Personnel Inaction - Rating: 3.0

open_threat:threat-name="TEC-001"

Organizational Fingerprinting via Open Sources - Rating:

open_threat:threat-name="TEC-002"

System Fingerprinting via Open Sources - Rating: 2.0

open_threat:threat-name="TEC-003"

System Fingerprinting via Scanning - Rating: 2.0

open_threat:threat-name="TEC-004"

System Fingerprinting via Sniffing - Rating: 2.0

open_threat:threat-name="TEC-005"

Credential Discovery via Open Sources - Rating: 4.0

open_threat:threat-name="TEC-006"

Credential Discovery via Scanning - Rating: 3.0

open_threat:threat-name="TEC-007"

Credential Discovery via Sniffing - Rating: 4.0

open_threat:threat-name="TEC-008"

Credential Discovery via Brute Force - Rating: 4.0

open_threat:threat-name="TEC-009"

Credential Discovery via Cracking - Rating: 4.0

open_threat:threat-name="TEC-010"

Credential Discovery via Guessing - Rating: 2.0

open_threat:threat-name="TEC-011"

Credential Discovery via Pre-Computational Attacks - Rating: 3.0

open_threat:threat-name="TEC-012"

Misuse of System Credentials - Rating: 3.0

open_threat:threat-name="TEC-013"

Escalation of Privilege - Rating: 5.0

open_threat:threat-name="TEC-014"

Abuse of System Privileges - Rating: 4.0

open_threat:threat-name="TEC-015"

Memory Manipulation - Rating: 4.0

open_threat:threat-name="TEC-016"

Cache Poisoning - Rating: 3.0

open_threat:threat-name="TEC-017"

Physical Manipulation of Technical Device - Rating: 2.0

open_threat:threat-name="TEC-018"

Manipulation of Trusted System - Rating: 4.0

open_threat:threat-name="TEC-019"

Cryptanalysis - Rating: 1.0

open_threat:threat-name="TEC-020"

Data Leakage / Theft - Rating: 3.0

open_threat:threat-name="TEC-021"

Denial of Service - Rating: 2.0

open_threat:threat-name="TEC-022"

Maintaining System Persistence - Rating: 5.0

open_threat:threat-name="TEC-023"

Manipulation of Data in Transit / Use - Rating: 2.0

open_threat:threat-name="TEC-024"

Capture of Data in Transit / Use via Sniffing - Rating: 3.0

open_threat:threat-name="TEC-025"

Capture of Data in Transit / Use via Debugging - Rating: 2.0

open_threat:threat-name="TEC-026"

Capture of Data in Transit / Use via Keystroke Logging - Rating: 3.0

open_threat:threat-name="TEC-027"

Replay of Data in Transit / Use - Rating: 2.0

open_threat:threat-name="TEC-028"

Misdelivery of Data - Rating: 2.0

open_threat:threat-name="TEC-029"

Capture of Stored Data - Rating: 3.0

open_threat:threat-name="TEC-030"

Manipulation of Stored Data - Rating: 3.0

open_threat:threat-name="TEC-031"

Application Exploitation via Input Manipulation - Rating: 5.0

open_threat:threat-name="TEC-032"

Application Exploitation via Parameter Injection - Rating: 4.0

open_threat:threat-name="TEC-033"

Application Exploitation via Code Injection - Rating: 4.0

open_threat:threat-name="TEC-034"

Application Exploitation via Command Injection - Rating: 4.0

open_threat:threat-name="TEC-035"

Application Exploitation via Path Traversal - Rating: 3.0

open_threat:threat-name="TEC-036"

Application Exploitation via API Abuse - Rating: 3.0

open_threat:threat-name="TEC-037"

Application Exploitation via Fuzzing - Rating: 3.0

open_threat:threat-name="TEC-038"

Application Exploitation via Reverse Engineering - Rating: 3.0

open_threat:threat-name="TEC-039"

Application Exploitation via Resource Location Guessing - Rating: 2.0

open_threat:threat-name="TEC-040"

Application Exploitation via Source Code Manipulation - Rating: 3.0

open_threat:threat-name="TEC-041"

Application Exploitation via Authentication Bypass - Rating: 2.0

osint

osint namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Open Source Intelligence - Classification (MISP taxonomies)

source-type

osint:source-type="blog-post"

Blog post

osint:source-type="microblog-post"

Microblog post like Twitter

osint:source-type="technical-report"

Technical or analysis report

osint:source-type="presentation"

Presentation or slidedeck

osint:source-type="news-report"

News report

osint:source-type="pastie-website"

Pastie-like website

osint:source-type="electronic-forum"

Electronic forum

osint:source-type="mailing-list"

Mailing-list

osint:source-type="block-or-filter-list"

Block or Filter List

osint:source-type="source-code-repository"

Source code repository

osint:source-type="expansion"

Expansion

osint:source-type="automatic-analysis"

Automatic analysis including dynamic analysis or sandboxes output

osint:source-type="automatic-collection"

Automatic collection including honeypots, spamtramps or equivalent technologies

osint:source-type="manual-analysis"

Manual analysis or investigation

osint:source-type="unknown"

Unknown

osint:source-type="other"

Other source not specified in this list

lifetime

osint:lifetime="perpetual"

Perpetual

Information available publicly on long-term

osint:lifetime="ephemeral"

Ephemeral

Information available publicly on short-term

certainty

osint:certainty="100"

Certainty (probability equals 1 - 100%)

Certainty

Associated numerical value="100"

osint:certainty="93"

Almost certain (probability equals 0.93 - 93%)

Almost certain

Associated numerical value="93"

osint:certainty="75"

Probable (probability equals 0.75 - 75%)

Probable

Associated numerical value="75"

osint:certainty="50"

Chances about even (probability equals 0.50 - 50%)

Chances about even

Associated numerical value="50"

osint:certainty="30"

Probably not (probability equals 0.30 - 30%)

Probably not

Associated numerical value="30"

osint:certainty="7"

Almost certainly not (probability equals 0.07 - 7%)

Almost certainly not

Associated numerical value="7"

osint:certainty="0"

Impossibility (probability equals 0 - 0%)

Impossibility

passivetotal

passivetotal namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Tags from RiskIQ's PassiveTotal service

sinkholed

passivetotal:sinkholed="yes"

Yes

passivetotal:sinkholed="no"

No

ever-comprimised

passivetotal:ever-comprimised="yes"

Yes

passivetotal:ever-comprimised="no"

No

dynamic-dns

passivetotal:dynamic-dns="yes"

Yes

passivetotal:dynamic-dns="no"

No

class

passivetotal:class="malicious"

Malicious

passivetotal:class="suspicious"

Malicious

passivetotal:class="non-malicious"

Non Malicious

passivetotal:class="unknown"

Unknown

pentest

pentest namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

pentest classification.

approach

This is group is dealing with differents types of pentest

pentest:approach="blackbox"

Blackbox penetration test requires no prior information about the target network or application and is actually performed keeping it as a real world hacker attack scenario. (https://www.evolution-sec.com/en/products/blackbox-penetration-testing)

pentest:approach="greybox"

Gray box testing lies between black and white. Testers will have knowledge of some areas but not others. These areas are defined at the start of an engagement.(https://www.intelisecure.com/security-assessments-pen-testing/approaches/)

pentest:approach="whitebox"

White box, or authenticated tests, target the security of your underlying technology with full knowledge of your IT department. Information typically shared with the tester includes: network diagrams, IP addresses, system configurations and access credentials.(https://www.intelisecure.com/security-assessments-pen-testing/approaches/)

pentest:approach="vulnerability_scanning"

Vulnerability scanning is a security technique used to identify security weaknesses in a computer system. (https://www.techopedia.com/definition/4160/vulnerability-scanning)

pentest:approach="redteam"

A red team is an group that challenges an organization to improve its effectiveness by assuming an adversarial role or point of view without any predefined scope. (https://en.wikipedia.org/wiki/Red_team)

scan

Automated tool that perform network checks

pentest:scan="vertical"

A scan against multiple ports of a single IP.

pentest:scan="horizontal"

A scan against a group of IPs for a single port.

pentest:scan="network_scan"

It is the discovery of networks and machines with services.

pentest:scan="vulnerability"

Vulnerability scanning is a security technique used to identify security weaknesses in a computer system. (https://www.techopedia.com/definition/4160/vulnerability-scanning)

exploit

Exploitation of a vulnerability

pentest:exploit="type confusion"

When a piece of code doesn't verify the type of object that is passed to it, and uses it blindly without type-checking, it leads to type confusion. (https://cloudblogs.microsoft.com/microsoftsecure/2015/06/17/understanding-type-confusion-vulnerabilities-cve-2015-0336/)

pentest:exploit="format_strings"

The format string exploit occurs when the submitted data of an input string leads to arbitrary read or write in the memory. In this way, the attacker could execute code, read the stack, or cause a segmentation fault in the running application, causing new behaviors that could compromise the security or the stability of the system. (https://www.owasp.org/index.php/Format_string_attack)

pentest:exploit="stack_overflow"

In software, a stack overflow is type of buffer overflow that occurs if the call stack pointer exceeds the stack bound. (https://en.wikipedia.org/wiki/Stack_overflow)

pentest:exploit="heap_overflow"

A heap overflow is a type of buffer overflow that occurs in the heap data area. (https://en.wikipedia.org/wiki/Heap_overflow)

pentest:exploit="heap_spraying"

Heap spraying is a technique used in exploits to facilitate arbitrary code execution. In general, code that sprays the heap attempts to put a certain sequence of bytes at a predetermined location in the memory of a target process by having it allocate (large) blocks on the process's heap and fill the bytes in these blocks with the right values. (https://en.wikipedia.org/wiki/Heap_spraying)

pentest:exploit="fuzzing"

Fuzzing is an automated software testing technique that involves providing invalid, unexpected, or random data as inputs to a computer program. (https://en.wikipedia.org/wiki/Fuzzing)

pentest:exploit="ROP"

The Return-Oriented Programming (ROP) is a computer security exploit technique in which the attacker uses control of the call stack to indirectly execute cherry-picked machine instructions or groups of machine instructions immediately prior to the return instruction in subroutines within the existing program code, in a way similar to the execution of a threaded code interpreter. (https://en.wikipedia.org/wiki/Return-oriented_programming)

pentest:exploit="null_pointer_dereference"

A NULL pointer dereference occurs when the application dereferences a pointer that it expects to be valid, but is NULL, typically causing a crash or exit. (https://cwe.mitre.org/data/definitions/476.html)

post_exploitation

Utilizing post exploitation techniques will ensure that a penetration tester maintains some level of access and can potentially lead to deeper footholds into the targets trusted infrastructure. (https://www.offensive-security.com/metasploit-unleashed/msf-post-exploitation/)

pentest:post_exploitation="privilege_escalation"

Privilege escalation is the act of exploiting a bug, design flaw or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user. (https://en.wikipedia.org/wiki/Privilege_escalation)

pentest:post_exploitation="pivoting"

Pivoting refers to a method used by penetration testers that uses the compromised system to attack other systems on the same network to avoid restrictions such as firewall configurations, which may prohibit direct access to all machines. (https://en.wikipedia.org/wiki/Exploit_(computer_security)#Pivoting)

pentest:post_exploitation="password_cracking"

Password cracking is the process of recovering passwords from data that have been stored in or transmitted by a computer system. (https://en.wikipedia.org/wiki/Password_cracking)

pentest:post_exploitation="persistence"

The persistence is when a penetration tester let him a way to keep its exploitation on a machine or a domain even if the system is rebooted.

pentest:post_exploitation="data_exfiltration"

After an exploitation of a machine, a penetration tester will try to exfiltrate sensitive data.

web

This is group is dealing with web vulnerabilities

pentest:web="injection"

Code injection is the exploitation of a computer bug that is caused by processing invalid data. Injection is used by an attacker to introduce (or "inject") code into a vulnerable computer program and change the course of execution. (https://en.wikipedia.org/wiki/Code_injection)

pentest:web="SQLi"

An SQL injection is a computer attack in which malicious code is embedded in a poorly-designed application and then passed to the SQL backend database. The malicious data then produces database query results or actions that should never have been executed.(https://www.techopedia.com/definition/4126/sql-injection)

pentest:web="NoSQLi"

An NoSQL injection is a computer attack in which malicious code is embedded in a poorly-designed application and then passed to the NoSQL backend database. The malicious data then produces database query results or actions that should never have been executed.

pentest:web="XML injection"

XML Injection is an attack technique used to manipulate or compromise the logic of an XML application or service. The injection of unintended XML content and/or structures into an XML

message can alter the intend logic of the application. Further, XML injection can cause the insertion of malicious content into the resulting message/document.(http://projects.webappsec.org/w/page/13247004/XML%20Injection)

pentest:web="CSRF"

Cross-Site Request Forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated. CSRF attacks specifically target state-changing requests, not theft of data, since the attacker has no way to see the response to the forged request.(https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF))

pentest:web="SSRF"

Server Side Request Forgery (SSRF) refers to an attack where in an attacker is able to send a crafted request from a vulnerable web application. SSRF is usually used to target internal systems behind firewalls that are normally inaccessible to an attacker from the external network. (https://www.acunetix.com/blog/articles/server-side-request-forgery-vulnerability/)

pentest:web="XSS"

Cross-site scripting (XSS) is a security breach that takes advantage of dynamically generated Web pages. In an XSS attack, a Web application is sent with a script that activates when it is read by an unsuspecting user's browser or by an application that has not protected itself against cross-site scripting. (https://www.webopedia.com/TERM/X/XSS.html)

pentest:web="file_inclusion"

The File Inclusion vulnerability allows an attacker to include a file, usually exploiting a "dynamic file inclusion" mechanisms implemented in the target application. The vulnerability occurs due to the use of user-supplied input without proper validation. (https://www.owasp.org/index.php/Testing_for_Local_File_Inclusion)

pentest:web="web_tree_discovery"

A web tree discovery is a brute force directories and files names on web/application server

pentest:web="bruteforce"

A brute-force attack consists of an attacker trying many passwords or passphrases with the hope of eventually guessing correctly. (https://en.wikipedia.org/wiki/Brute-force_attack)

pentest:web="fuzzing"

Fuzzing is an automated software testing technique that involves providing invalid, unexpected, or random data as inputs to a computer program. (https://en.wikipedia.org/wiki/Fuzzing)

network

This is group is dealing with network vulnerabilities

pentest:network="sniffing"

Sniffing involves capturing, decoding, inspecting and interpreting the information inside a network packet on a TCP/IP network. (http://www.valencynetworks.com/articles/cyber-security-attacks-network-sniffing.html)

pentest:network="spoofing"

Spoofing, in general, is a fraudulent or malicious practice in which communication is sent from an unknown source disguised as a source known to the receiver. Spoofing is most prevalent in communication mechanisms that lack a high level of security. (https://www.techopedia.com/definition/5398/spoofing)

pentest:network="man_in_the_middle"

man-in-the-middle attack (MITM) is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other. (https://en.wikipedia.org/wiki/Man-in-the-middle_attack)

pentest:network="network_discovery"

It is the discovery of networks and machines with services.

social_engineering

Social engineering is an attack vector that relies heavily on human interaction and often involves tricking people into breaking normal security procedures. (https://krashconsulting.com/index.php/services/sea/)

pentest:social_engineering="phishing"

Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication. (https://en.wikipedia.org/wiki/Phishing)

pentest:social_engineering="malware"

Malware, short for malicious software, is an umbrella term used to refer to a variety of forms of harmful or intrusive software, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware, and other malicious programs. (https://en.wikipedia.org/wiki/Malware)

vulnerability

This is group is dealing with the classification of weaknesses and vulnerabilities

pentest:vulnerability="CWE"

Targeted to developers and security practitioners, the Common Weakness Enumeration (CWE) is a formal list of software weakness types. (https://cwe.mitre.org/about/)

pentest:vulnerability="CVE"

Common Vulnerabilities and Exposures (CVE) is a dictionary-type list of standardized names for vulnerabilities and other information related to security exposures. (https://en.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures)

priority-level

priority-level namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

After an incident is scored, it is assigned a priority level. The six levels listed below are aligned with NCCIC, DHS, and the CISS to help provide a common lexicon when discussing incidents. This priority assignment drives NCCIC urgency, pre-approved incident response offerings, reporting requirements, and recommendations for leadership escalation. Generally, incident priority distribution should follow a similar pattern to the graph below. Based on https://www.us-cert.gov/NCCIC-Cyber-Incident-Scoring-System.

Exclusive flag set which means the values or predicate below must be set exclusively.

emergency

An Emergency priority incident poses an imminent threat to the provision of wide-scale critical infrastructure services, national government stability, or the lives of U.S. persons.

priority-level:emergency

Emergency

An Emergency priority incident poses an imminent threat to the provision of wide-scale critical infrastructure services, national government stability, or the lives of U.S. persons.

100

severe

A Severe priority incident is likely to result in a significant impact to public health or safety, national security, economic security, foreign relations, or civil liberties.

priority-level:severe

Severe

A Severe priority incident is likely to result in a significant impact to public health or safety, national security, economic security, foreign relations, or civil liberties.

90

high

A High priority incident is likely to result in a demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.

priority-level:high

High

A High priority incident is likely to result in a demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.

85

medium

A Medium priority incident may affect public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.

priority-level:medium

Medium

A Medium priority incident may affect public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.

75

low

A Low priority incident is unlikely to affect public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.

priority-level:low

Low

A Low priority incident is unlikely to affect public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.

50

baseline-minor

A Baseline–Minor priority incident is an incident that is highly unlikely to affect public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence. The potential for impact, however, exists and warrants additional scrutiny.

priority-level:baseline-minor

Baseline - Minor

A Baseline–Minor priority incident is an incident that is highly unlikely to affect public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence. The potential for impact, however, exists and warrants additional scrutiny.

25

baseline-negligible

A Baseline–Negligible priority incident is an incident that is highly unlikely to affect public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.

priority-level:baseline-negligible

Baseline - Negligible

A Baseline–Negligible priority incident is an incident that is highly unlikely to affect public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.

rt_event_status

rt_event_status namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Status of events used in Request Tracker.

event-status

rt_event_status:event-status="new"

New

rt_event_status:event-status="open"

Open

rt_event_status:event-status="stalled"

Stalled

rt_event_status:event-status="rejected"

rejected

rt_event_status:event-status="resolved"

Resolved

rt_event_status:event-status="deleted"

Deleted

runtime-packer

runtime-packer namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Runtime or software packer used to combine compressed data with the decompression code. The decompression code can add additional obfuscations mechanisms including polymorphic-packer or other obfuscation techniques. This taxonomy lists all the known or official packer used for legitimate use or for packing malicious binaries.

portable-executable

runtime-packer:portable-executable=".netshrink"

runtime-packer:portable-executable="armadillo"

netshrink

Armadillo

runtime-packer:portable-executable="aspack"

ASPack

runtime-packer:portable-executable="aspr-asprotect"

ASPR (ASProtect)

runtime-packer:portable-executable="boxedapp-packer"

BoxedApp Packer

runtime-packer:portable-executable="cexe"

CExe

runtime-packer:portable-executable="dotbundle"

dotBundle

runtime-packer:portable-executable="enigma-protector"

Enigma Protector

runtime-packer:portable-executable="exe-bundle"

EXE Bundle

runtime-packer:portable-executable="exe-stealth"

EXE Stealth

runtime-packer:portable-executable="expressor"

eXPressor

runtime-packer:portable-executable="fsg"

FSG

runtime-packer:portable-executable="kkrunchy-src"

kkrunchy src

runtime-packer:portable-executable="mew"

MEW

runtime-packer:portable-executable="mpress"

MPRESS

runtime-packer:portable-executable="obsidium"

Obsidium

runtime-packer:portable-executable="pelock"

PELock

runtime-packer:portable-executable="pespin"

PESpin

runtime-packer:portable-executable="petite"

Petite

runtime-packer:portable-executable="rlpack-basic"

RLPack Basic

runtime-packer:portable-executable="smart-packer-pro"

Smart Packer Pro

runtime-packer:portable-executable="themida"

Themida

runtime-packer:portable-executable="upx"

UPX

runtime-packer:portable-executable="vmprotect"

VMProtect

runtime-packer:portable-executable="xcomp-xpack"

XComp/XPack

elf

cli-assembly

stealth_malware

stealth_malware namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Classification based on malware stealth techniques. Described in https://vxheaven.org/lib/pdf/Introducing%20Stealth%20Malware%20Taxonomy.pdf

type

stealth_malware:type="0"

No OS or system compromise. The malware runs as a normal user process using only official API calls.

stealth_malware:type="I"

The malware modifies constant sections of the kernel and/or processes such as code sections.

stealth_malware:type="II"

The malware does not modify constant sections but only the dynamic sections of the kernel and/or processes such as data sections.

stealth_malware:type="III"

The malware does not modify any sections of the kernel and/or processes but influences the system without modifying the OS. For example using hardware virtualization techniques.

stix-ttp

stix-ttp namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

TTPs are representations of the behavior or modus operandi of cyber adversaries.

victim-targeting

stix-ttp:victim-targeting="business-professional-sector"

Business & Professional Services Sector

stix-ttp:victim-targeting="retail-sector"

Retail Sector

stix-ttp:victim-targeting="financial-sector"

Financial Services Sector

stix-ttp:victim-targeting="media-entertainment-sector"

Media & Entertainment Sector

stix-ttp:victim-targeting="construction-engineering-sector"

Construction & Engineering Sector

stix-ttp:victim-targeting="government-international-organizations-sector"

Goverment & International Organizations

stix-ttp:victim-targeting="legal-sector"

Legal Services

stix-ttp:victim-targeting="hightech-it-sector"

High-Tech & IT Sector

stix-ttp:victim-targeting="healthcare-sector"

Healthcare Sector

stix-ttp:victim-targeting="transportation-sector"

Transportation Sector

stix-ttp:victim-targeting="aerospace-defence-sector"

Aerospace & Defense Sector

stix-ttp:victim-targeting="energy-sector"

Energy Sector

stix-ttp:victim-targeting="food-sector"

Food Sector

stix-ttp:victim-targeting="natural-resources-sector"

Natural Resources Sector

stix-ttp:victim-targeting="other-sector"

Other Sector

stix-ttp:victim-targeting="corporate-employee-information"

Corporate Employee Information

stix-ttp:victim-targeting="customer-pii"

Customer PII

stix-ttp:victim-targeting="email-lists-archives"

Email Lists/Archives

stix-ttp:victim-targeting="financial-data"

Financial Data

stix-ttp:victim-targeting="intellectual-property"

Intellectual Property

stix-ttp:victim-targeting="mobile-phone-contacts"

Mobile Phone Contacts

stix-ttp:victim-targeting="user-credentials"

User Credentials

stix-ttp:victim-targeting="authentification-cookies"

Authentication Cookies

targeted-threat-index

targeted-threat-index namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

The Targeted Threat Index is a metric for assigning an overall threat ranking score to email messages that deliver malware to a victim's computer. The TTI metric was first introduced at

SecTor 2013 by Seth Hardy as part of the talk “RATastrophe: Monitoring a Malware Menagerie” along with Katie Kleemola and Greg Wiseman.

targeting-sophistication-base-value

The base value of the score ranges from 0 to 5, based on the sophistication of the email’s social engineering techniques used to get the victim to open the attachment. This score considers the content and presentation of the message as well as the claimed sender identity. This determination also includes the content of any associated files; many times malware is injected into legitimate relevant documents.

targeted-threat-index:targeting-sophistication-base-value="not-targeted"

Not targeted, e.g. spam or financially motivated malware.

targeted-threat-index:targeting-sophistication-base-value="targeted-but-not-customized"

Targeted but not customized. Sent with a message that is obviously false with little to no validation required.

Associated numerical value="1"

targeted-threat-index:targeting-sophistication-base-value="targeted-and-poorly-customized"

Targeted and poorly customized. Content is generally relevant to the target. May look questionable.

Associated numerical value="2"

targeted-threat-index:targeting-sophistication-base-value="targeted-and-customized"

Targeted and customized. May use a real person/organization or content to convince the target the message is legitimate. Content is specifically relevant to the target and looks legitimate.

Associated numerical value="3"

targeted-threat-index:targeting-sophistication-base-value="targeted-and-well-customized"

Targeted and well-customized. Uses a real person/organization and content to convince the target the message is legitimate. Probably directly addressing the recipient. Content is specifically relevant to the target, looks legitimate, and can be externally referenced (e.g. by a website). May be sent from a hacked account.

Associated numerical value="4"

targeted-threat-index:targeting-sophistication-base-value="targeted-and-highly-customized-using-sensitive-data"

Targeted and highly customized using sensitive data. Individually targeted and customized, likely using inside/sensitive information that is directly relevant to the target.

Associated numerical value="5"

technical-sophistication-multiplier

The technical sophistication score is a multiplier ranging from 1 to 2 based on how advanced the associated malware is, including malicious file attachments as well as links to malware hosted on another system. We use a multiplier because advanced malware requires significantly more effort and time (or money, in the case of commercial solutions) to custom-tune for a particular target.

targeted-threat-index:technical-sophistication-multiplier="the-sample-contains-no code-protection"

The sample contains no code protection such as packing, obfuscation (e.g. simple rotation of C2 names or other interesting strings), or anti-reversing tricks.

Associated numerical value="1"

targeted-threat-index:technical-sophistication-multiplier="the-sample-contains-a-simple-method-of-protection"

The sample contains a simple method of protection, such as one of the following: code protection using publicly available tools where the reverse method is available, such as UPX packing; simple anti-reversing techniques such as not using import tables, or a call to IsDebuggerPresent(); self-disabling in the presence of AV software.

Associated numerical value="1.25"

targeted-threat-index:technical-sophistication-multiplier="the-sample-contains-multiple-minor-code-protection-techniques"

The sample contains multiple minor code protection techniques (anti-reversing tricks, packing, VM / reversing tools detection) that require some low-level knowledge. This level includes malware where code that contains the core functionality of the program is decrypted only in memory.

Associated numerical value="1.5"

targeted-threat-index:technical-sophistication-multiplier="the-sample-contains-minor-code-protection-techniques-plus-one-advanced"

The sample contains minor code protection techniques along with at least one advanced protection method such as rootkit functionality or a custom virtualized packer.

Associated numerical value="1.75"

targeted-threat-index:technical-sophistication-multiplier="the-sample-contains-multiple-advanced-protection-techniques"

The sample contains multiple advanced protection techniques, e.g. rootkit capability, virtualized packer, multiple anti-reversing techniques, and is clearly designed by a professional software engineering team.

Associated numerical value="2"

tlp

tlp namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

The Traffic Light Protocol - or short: TLP - was designed with the objective to create a favorable classification scheme for sharing sensitive information while keeping the control over its distribution at the same time.

Exclusive flag set which means the values or predicate below must be set exclusively.

red

Not for disclosure, restricted to participants only. Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused. Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.

tlp:red

(TLP:RED) Information exclusively and directly given to (a group of) individual recipients. Sharing outside is not legitimate.

Not for disclosure, restricted to participants only. Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused. Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.

amber

Limited disclosure, restricted to participants' organizations. Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation,

or operations if shared outside of the organizations involved. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.

tlp:amber

(TLP:AMBER) Information exclusively given to an organization; sharing limited within the organization to be effectively acted upon.

Limited disclosure, restricted to participants' organizations. Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.

green

Limited disclosure, restricted to the community. Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.

tlp:green

(TLP:GREEN) Information given to a community or a group of organizations at large. The information cannot be publicly released.

Limited disclosure, restricted to the community. Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.

white

Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

tlp:white

(TLP:WHITE) Information can be shared publicly in accordance with the law.

Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

ex:chr

tlp:ex:chr

(TLP:EX:CHR) Information extended with a specific tag called Chatham House Rule (CHR). When this specific CHR tag is mentioned, the attribution (the source of information) must not be disclosed. This additional rule is at the discretion of the initial sender who can decide to apply or not the CHR tag.

tor

tor namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Taxonomy to describe Tor network infrastructure

tor-relay-type

tor:tor-relay-type="entry-guard-relay"

Entry node to the Tor network

tor:tor-relay-type="middle-relay"

Tor node relaying traffic between an entry-guard-relay to an exit-relay

tor:tor-relay-type="exit-relay"

Tor node relaying traffic outside of the Tor network to the original destination

tor:tor-relay-type="bridge-relay"

Entry node to the Tor network - partially unpublished

veris

veris namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Vocabulary for Event Recording and Incident Sharing (VERIS)

iso_currency_code

veris:iso_currency_code="DZD"

DZD - Algerian Dinar

veris:iso_currency_code="NAD"

NAD - Namibia Dollar

veris:iso_currency_code="GHS"

GHS - Ghana Cedi

veris:iso_currency_code="EGP"

EGP - Egyptian Pound

veris:iso_currency_code="BGN"

BGN - Bulgarian Lev

veris:iso_currency_code="PAB"

PAB - Balboa

veris:iso_currency_code="BOB"

BOB - Boliviano

veris:iso_currency_code="DKK"

DKK - Danish Krone

veris:iso_currency_code="BWP"

BWP - Pula

veris:iso_currency_code="LBP"

LBP - Lebanese Pound

veris:iso_currency_code="TZS"

TZS - Tanzanian Shilling

veris:iso_currency_code="VND"

VND - Dong

veris:iso_currency_code="AOA"

AOA - Kwanza

veris:iso_currency_code="KHR"

KHR - Riel

veris:iso_currency_code="MYR"

MYR - Malaysian Ringgit

veris:iso_currency_code="KYD"

KYD - Cayman Islands Dollar

veris:iso_currency_code="LYD"

LYD - Libyan Dinar

veris:iso_currency_code="UAH"

UAH - Hryvnia

veris:iso_currency_code="JOD"

JOD - Jordanian Dinar

veris:iso_currency_code="AWG"

AWG - Aruban Florin

veris:iso_currency_code="SAR"

SAR - Saudi Riyal

veris:iso_currency_code="EUR"

EUR - Euro

veris:iso_currency_code="HKD"

HKD - Hong Kong Dollar

veris:iso_currency_code="CHF"

CHF - Swiss Franc

veris:iso_currency_code="GIP"

GIP - Gibraltar Pound

veris:iso_currency_code="BYR"

BYR - Belarussian Ruble

veris:iso_currency_code="ALL"

ALL - Lek

veris:iso_currency_code="MRO"

MRO - Ouguiya

veris:iso_currency_code="HRK"

HRK - Croatian Kuna

veris:iso_currency_code="DJF"

DJF - Djibouti Franc

veris:iso_currency_code="SZL"

SZL - Lilangeni

veris:iso_currency_code="THB"

THB - Baht

veris:iso_currency_code="XAF"

XAF - CFA Franc BEAC

veris:iso_currency_code="BND"

BND - Brunei Dollar

veris:iso_currency_code="ISK"

ISK - Iceland Krona

veris:iso_currency_code="UYU"

UYU - Peso Uruguayo

veris:iso_currency_code="NIO"

NIO - Cordoba Oro

veris:iso_currency_code="LAK"

LAK - Kip

veris:iso_currency_code="SYP"

SYP - Syrian Pound

veris:iso_currency_code="MAD"

MAD - Moroccan Dirham

veris:iso_currency_code="MZN"

MZN - Mozambique Metical

veris:iso_currency_code="PHP"

PHP - Philippine Peso

veris:iso_currency_code="ZAR"

ZAR - South African Rand

veris:iso_currency_code="NPR"

NPR - Nepalese Rupee

veris:iso_currency_code="NGN"

NGN - Naira

veris:iso_currency_code="ZWD"

ZWD - Zimbabwean Dollar A/06

veris:iso_currency_code="CRC"

CRC - Costa Rican Colon

veris:iso_currency_code="AED"

AED - UAE Dirham

veris:iso_currency_code="GBP"

GBP - Pound Sterling

veris:iso_currency_code="MWK"

MWK - Kwacha

veris:iso_currency_code="LKR"

LKR - Sri Lanka Rupee

veris:iso_currency_code="PKR"

PKR - Pakistan Rupee

veris:iso_currency_code="HUF"

HUF - Forint

veris:iso_currency_code="BMD"

BMD - Bermudian Dollar

veris:iso_currency_code="LSL"

LSL - Loti

veris:iso_currency_code="MNT"

MNT - Tugrik

veris:iso_currency_code="AMD"

AMD - Armenian Dram

veris:iso_currency_code="UGX"

UGX - Uganda Shilling

veris:iso_currency_code="QAR"

QAR - Qatari Rial

veris:iso_currency_code="XDR"

XDR - SDR (Special Drawing Right)

veris:iso_currency_code="JMD"

JMD - Jamaican Dollar

veris:iso_currency_code="GEL"

GEL - Lari

veris:iso_currency_code="SHP"

SHP - Saint Helena Pound

veris:iso_currency_code="AFN"

AFN - Afghani

veris:iso_currency_code="SBD"

SBD - Solomon Islands Dollar

veris:iso_currency_code="KPW"

KPW - North Korean Won

veris:iso_currency_code="TRY"

TRY - Turkish Lira

veris:iso_currency_code="BDT"

BDT - Taka

veris:iso_currency_code="YER"

YER - Yemeni Rial

veris:iso_currency_code="HTG"

HTG - Gourde

veris:iso_currency_code="XOF"

XOF - CFA Franc BCEAO

veris:iso_currency_code="MGA"

MGA - Malagasy Ariary

veris:iso_currency_code="ANG"

ANG - Netherlands Antillean Guilder

veris:iso_currency_code="LRD"

LRD - Liberian Dollar

veris:iso_currency_code="RWF"

RWF - Rwanda Franc

veris:iso_currency_code="NOK"

NOK - Norwegian Krone

veris:iso_currency_code="MOP"

MOP - Pataca

veris:iso_currency_code="INR"

INR - Indian Rupee

veris:iso_currency_code="MXN"

MXN - Mexican Peso

veris:iso_currency_code="CZK"

CZK - Czech Koruna

veris:iso_currency_code="TJS"

TJS - Somoni

veris:iso_currency_code="TWD"

TWD - New Taiwan Dollar

veris:iso_currency_code="BTN"

BTN - Ngultrum

veris:iso_currency_code="COP"

COP - Colombian Peso

veris:iso_currency_code="TMT"

TMT - Turkmenistan New Manat

veris:iso_currency_code="MUR"

MUR - Mauritius Rupee

veris:iso_currency_code="IDR"

IDR - Rupiah

veris:iso_currency_code="HNL"

HNL - Lempira

veris:iso_currency_code="XPF"

XPF - CFP Franc

veris:iso_currency_code="FJD"

FJD - Fiji Dollar

veris:iso_currency_code="ETB"

ETB - Ethiopian Birr

veris:iso_currency_code="PEN"

PEN - Nuevo Sol

veris:iso_currency_code="BZD"

BZD - Belize Dollar

veris:iso_currency_code="ILS"

ILS - New Israeli Sheqel

veris:iso_currency_code="DOP"

DOP - Dominican Peso

veris:iso_currency_code="GGP"

GGP - Guernsey pound

veris:iso_currency_code="MDL"

MDL - Moldovan Leu

veris:iso_currency_code="BSD"

BSD - Bahamian Dollar

veris:iso_currency_code="SPL"

SPL - Seborga Luigino

veris:iso_currency_code="SEK"

SEK - Swedish Krona

veris:iso_currency_code="ZMK"

ZMK - Zambian Kwacha

veris:iso_currency_code="JEP"

JEP - Jersey pound

veris:iso_currency_code="AUD"

AUD - Australian Dollar

veris:iso_currency_code="SRD"

SRD - Surinam Dollar

veris:iso_currency_code="CUP"

CUP - Cuban Peso

veris:iso_currency_code="BBD"

BBD - Barbados Dollar

veris:iso_currency_code="KMF"

KMF - Comoro Franc

veris:iso_currency_code="KRW"

KRW - South Korean Won

veris:iso_currency_code="GMD"

GMD - Dalasi

veris:iso_currency_code="VEF"

VEF - Bolivar

veris:iso_currency_code="IMP"

IMP - Isle of Man Pound

veris:iso_currency_code="CUC"

CUC - Peso Convertible

veris:iso_currency_code="TVD"

TVD - Tuvalu Dollar

veris:iso_currency_code="CLP"

CLP - Chilean Peso

veris:iso_currency_code="LTL"

LTL - Lithuanian Litas

veris:iso_currency_code="CDF"

CDF - Congolese Franc

veris:iso_currency_code="XCD"

XCD - East Caribbean Dollar

veris:iso_currency_code="KZT"

KZT - Tenge

veris:iso_currency_code="RUB"

RUB - Russian Ruble

veris:iso_currency_code="TTD"

TTD - Trinidad and Tobago Dollar

veris:iso_currency_code="OMR"

OMR - Rial Omani

veris:iso_currency_code="BRL"

BRL - Brazilian Real

veris:iso_currency_code="MMK"

MMK - Kyat

veris:iso_currency_code="PLN"

PLN - Zloty

veris:iso_currency_code="PYG"

PYG - Guarani

veris:iso_currency_code="KES"

KES - Kenyan Shilling

veris:iso_currency_code="SVC"

SVC - El Salvador Colon

veris:iso_currency_code="MKD"

MKD - Denar

veris:iso_currency_code="AZN"

AZN - Azerbaijanian Manat

veris:iso_currency_code="TOP"

TOP - Pa’anga

veris:iso_currency_code="MVR"

MVR - Rufiyaa

veris:iso_currency_code="VUV"

VUV - Vatu

veris:iso_currency_code="GNF"

GNF - Guinea Franc

veris:iso_currency_code="WST"

WST - Tala

veris:iso_currency_code="IQD"

IQD - Iraqi Dinar

veris:iso_currency_code="ERN"

ERN - Nakfa

veris:iso_currency_code="BAM"

BAM - Convertible Mark

veris:iso_currency_code="SCR"

SCR - Seychelles Rupee

veris:iso_currency_code="CAD"

CAD - Canadian Dollar

veris:iso_currency_code="CVE"

CVE - Cape Verde Escudo

veris:iso_currency_code="KWD"

KWD - Kuwaiti Dinar

veris:iso_currency_code="BIF"

BIF - Burundi Franc

veris:iso_currency_code="PGK"

PGK - Kina

veris:iso_currency_code="SOS"

SOS - Somali Shilling

veris:iso_currency_code="SGD"

SGD - Singapore Dollar

veris:iso_currency_code="UZS"

UZS - Uzbekistan Sum

veris:iso_currency_code="STD"

STD - Dobra

veris:iso_currency_code="IRR"

IRR - Iranian Rial

veris:iso_currency_code="CNY"

CNY - Yuan Renminbi

veris:iso_currency_code="SLL"

SLL - Leone

veris:iso_currency_code="TND"

TND - Tunisian Dinar

veris:iso_currency_code="GYD"

GYD - Guyana Dollar

veris:iso_currency_code="NZD"

NZD - New Zealand Dollar

veris:iso_currency_code="FKP"

FKP - Falkland Islands Pound

veris:iso_currency_code="LVL"

LVL - Latvian Lats

veris:iso_currency_code="USD"

USD - US Dollar

veris:iso_currency_code="KGS"

KGS - Som

veris:iso_currency_code="ARS"

ARS - Argentine Peso

veris:iso_currency_code="RON"

RON - New Romanian Leu

veris:iso_currency_code="GTQ"

GTQ - Quetzal

veris:iso_currency_code="RSD"

RSD - Serbian Dinar

veris:iso_currency_code="BHD"

BHD - Bahraini Dinar

veris:iso_currency_code="JPY"

JPY - Yen

veris:iso_currency_code="SDG"

SDG - Sudanese Pound

confidence

veris:confidence="High"

High confidence

veris:confidence="None"

No confidence

veris:confidence="Medium"

Medium confidence

veris:confidence="Low"

Low confidence

targeted

veris:targeted="Targeted"

Targeted: victim chosen as target then actor determined what weaknesses could be exploited

veris:targeted="NA"

Not applicable

veris:targeted="Opportunistic"

Opportunistic: victim attacked because they exhibited a weakness the actor knew how to exploit

veris:targeted="Unknown"

Unknown

discovery_method

veris:discovery_method="Int - financial audit"

Internal - financial audit and reconciliation process

veris:discovery_method="Ext - found documents"

External - Found documents

veris:discovery_method="Unknown"

Unknown

veris:discovery_method="Ext - audit"

External - security audit or scan

veris:discovery_method="Ext - incident response"

External - Notified while investigating another incident

veris:discovery_method="Ext - unknown"

External - unknown

veris:discovery_method="Other"

Other

veris:discovery_method="Int - NIDS"

Internal - network IDS or IPS alert

veris:discovery_method="Ext - emergency response team"

External - Emergency response team

veris:discovery_method="Ext - fraud detection"

External - fraud detection (e.g., CPP)

veris:discovery_method="Int - incident response"

Internal - discovered while responding to another (separate) incident

veris:discovery_method="Ext - customer"

External - reported by customer or partner affected by the incident

veris:discovery_method="Prt - audit"

Partner - Audit performed by a partner organization

veris:discovery_method="Int - IT review"

Internal - Informal IT review

veris:discovery_method="Int - log review"

Internal - log review process or SIEM

veris:discovery_method="Int - unknown"

Internal - unknown

veris:discovery_method="Ext - suspicious traffic"

External - Report of suspicious traffic

veris:discovery_method="Int - HIDS"

Internal - host IDS or file integrity monitoring

veris:discovery_method="Prt - Other"

Partner - Other

veris:discovery_method="Ext - monitoring service"

External - managed security event monitoring service

veris:discovery_method="Prt - antivirus"

Partner - Notified by antivirus company but not through AV product

veris:discovery_method="Prt - Unknown"

Partner - Unknown

veris:discovery_method="Int - security alarm"

Internal - physical security system alarm

veris:discovery_method="Ext - law enforcement"

Internal - notified by law enforcement or government agency

veris:discovery_method="Int - antivirus"

Internal - antivirus alert

veris:discovery_method="Int - infrastructure monitoring"

Internal - Infrastructure monitoring

veris:discovery_method="Prt - incident response"

Partner - notified while investigating another incident

veris:discovery_method="Int - data loss prevention"

Internal - Data loss prevention software

veris:discovery_method="Int - fraud detection"

Internal - fraud detection mechanism

veris:discovery_method="Prt - monitoring service"

Partner - Reported by a monitoring service

veris:discovery_method="Int - reported by employee"

Internal - reported by employee who saw something odd

veris:discovery_method="Ext - actor disclosure"

External - disclosed by threat agent (e.g., public brag, private blackmail)

cost_corrective_action

veris:cost_corrective_action="Simple and cheap"

Simple and cheap

veris:cost_corrective_action="Unknown"

Unknown

veris:cost_corrective_action="Something in-between"

Something in-between

veris:cost_corrective_action="Difficult and expensive"

Difficult and expensive

security_incident

veris:security_incident="Suspected"

Suspected

veris:security_incident="Confirmed"

Yes - Confirmed

veris:security_incident="Near miss"

Near miss (actions did not compromise asset)

veris:security_incident="False positive"

False positive (response triggered, but no incident)

country

veris:country="BD"

Bangladesh

veris:country="BE"

Belgium

veris:country="BF"

Burkina Faso

veris:country="BG"

Bulgaria

veris:country="BA"

Bosnia and Herzegovina

veris:country="BB"

Barbados

veris:country="WF"

Wallis and Futuna Islands

veris:country="BL"

Saint-Barthelemy

veris:country="BM"

Bermuda

veris:country="BN"

Brunei Darussalam

veris:country="BO"

Bolivia

veris:country="BH"

Bahrain

veris:country="BI"

Burundi

veris:country="BJ"

Benin

veris:country="BT"

Bhutan

veris:country="JM"

Jamaica

veris:country="BV"

Bouvet Island

veris:country="BW"

Botswana

veris:country="WS"

Samoa

veris:country="BQ"

Bonaire, Saint Eustatius and Saba

veris:country="BR"

Brazil

veris:country="BS"

Bahamas

veris:country="JE"

Jersey

veris:country="BY"

Belarus

veris:country="BZ"

Belize

veris:country="RU"

Russian Federation

veris:country="RW"

Rwanda

veris:country="RS"

Serbia

veris:country="TL"

Timor-Leste

veris:country="RE"

Reunion

veris:country="TM"

Turkmenistan

veris:country="Unknown"

Unknown

veris:country="TJ"

Tajikistan

veris:country="RO"

Romania

veris:country="TK"

Tokelau

veris:country="GW"

Guinea-Bissau

veris:country="GU"

Guam

veris:country="GT"

Guatemala

veris:country="GS"

South Georgia and the South Sandwich Islands

veris:country="GR"

Greece

veris:country="GQ"

Equatorial Guinea

veris:country="GP"

Guadeloupe

veris:country="JP"

Japan

veris:country="GY"

Guyana

veris:country="GG"

Guernsey

veris:country="GF"

French Guiana

veris:country="GE"

Georgia

veris:country="GD"

Grenada

veris:country="GB"

United Kingdom

veris:country="GA"

Gabon

veris:country="SV"

El Salvador

veris:country="GN"

Guinea

veris:country="GM"

Gambia

veris:country="GL"

Greenland

veris:country="GI"

Gibraltar

veris:country="GH"

Ghana

veris:country="OM"

Oman

veris:country="TN"

Tunisia

veris:country="JO"

Jordan

veris:country="HR"

Croatia

veris:country="HT"

Haiti

veris:country="HU"

Hungary

veris:country="HK"

Hong Kong

veris:country="HN"

Honduras

veris:country="HM"

Heard Island and McDonal Islands

veris:country="VE"

Venezuela (Bolivarian Republic of)

veris:country="PR"

Puerto Rico

veris:country="PS"

Palestinian Territory, Occupied

veris:country="PW"

Palau

veris:country="PT"

Portugal

veris:country="SJ"

Svalbard and Jan Mayen Islands

veris:country="PY"

Paraguay

veris:country="IQ"

Iraq

veris:country="PA"

Panama

veris:country="PF"

French Polynesia

veris:country="PG"

Papua New Guinea

veris:country="PE"

Peru

veris:country="PK"

Pakistan

veris:country="PH"

Philippines

veris:country="PN"

Pitcairn

veris:country="PL"

Poland

veris:country="PM"

Saint Pierre and Miquelon

veris:country="ZM"

Zambia

veris:country="EH"

Western Sahara

veris:country="EE"

Estonia

veris:country="EG"

Egypt

veris:country="ZA"

South Africa

veris:country="EC"

Ecuador

veris:country="IT"

Italy

veris:country="VN"

Viet Nam

veris:country="SB"

Solomon Islands

veris:country="ET"

Ethiopia

veris:country="SO"

Somalia

veris:country="ZW"

Zimbabwe

veris:country="SA"

Saudi Arabia

veris:country="ES"

Spain

veris:country="ER"

Eritrea

veris:country="ME"

Montenegro

veris:country="MD"

Moldova, Republic of

veris:country="MG"

Madagascar

veris:country="MF"

Saint Martin (French part)

veris:country="MA"

Morocco

veris:country="MC"

Monaco

veris:country="UZ"

Uzbekistan

veris:country="MM"

Myanmar

veris:country="ML"

Mali

veris:country="MO"

Macao

veris:country="MN"

Mongolia

veris:country="MH"

Marshall Islands

veris:country="MK"

Macedonia, The former Yugoslav Republic of

veris:country="MU"

Mauritius

veris:country="MT"

Malta

veris:country="MW"

Malawi

veris:country="MV"

Maldives

veris:country="MQ"

Martinique

veris:country="MP"

Northern Mariana Islands

veris:country="MS"

Montserrat

veris:country="MR"

Mauritania

veris:country="IM"

Isle of Man

veris:country="UG"

Uganda

veris:country="TZ"

Tanzania, United Republic of

veris:country="MY"

Malaysia

veris:country="MX"

Mexico

veris:country="IL"

Israel

veris:country="FR"

France

veris:country="IO"

British Virgin Islands

veris:country="SH"

Saint Helena

veris:country="FI"

Finland

veris:country="FJ"

Fiji

veris:country="FK"

Faeroe Islands

veris:country="FM"

Micronesia (Federated States of)

veris:country="FO"

Falkland Islands (Malvinas)

veris:country="NI"

Nicaragua

veris:country="NL"

Netherlands

veris:country="NO"

Norway

veris:country="NA"

Namibia

veris:country="VU"

Vanuatu

veris:country="NC"

New Caledonia

veris:country="NE"

Niger

veris:country="NF"

Norfolk Island

veris:country="NG"

Nigeria

veris:country="NZ"

New Zealand

veris:country="NP"

Nepal

veris:country="NR"

Nauru

veris:country="NU"

Niue

veris:country="CK"

Cook Islands

veris:country="CI"

Cote d’Ivoire

veris:country="CH"

Switzerland

veris:country="CO"

Colombia

veris:country="CN"

China

veris:country="CM"

Cameroon

veris:country="CL"

Chile

veris:country="CC"

Cocos (Keeling) Islands

veris:country="CA"

Canada

veris:country="CG"

Congo

veris:country="CF"

Central African Republic

veris:country="CD"

Congo, Democratic Republic of the

veris:country="CZ"

Czech Republic

veris:country="CY"

Cyprus

veris:country="CX"

Christmas Island

veris:country="CR"

Costa Rica

veris:country="CW"

Curacao

veris:country="CV"

Cape Verde

veris:country="CU"

Cuba

veris:country="SZ"

Swaziland

veris:country="SY"

Syrian Arab Republic

veris:country="SX"

Sint Maarten (Dutch part)

veris:country="KG"

Kyrgyzstan

veris:country="KE"

Kenya

veris:country="SS"

South Sudan

veris:country="SR"

Suriname

veris:country="KI"

Kiribati

veris:country="KH"

Cambodia

veris:country="KN"

Saint Kitts and Nevis

veris:country="KM"

Comoros

veris:country="ST"

Sao Tome and Principe

veris:country="SK"

Slovakia

veris:country="KR"

Korea, Republic of

veris:country="SI"

Slovenia

veris:country="KP"

Korea, Democratic People’s Republic of

veris:country="KW"

Kuwait

veris:country="SN"

Senegal

veris:country="SM"

San Marino

veris:country="SL"

Sierra Leone

veris:country="SC"

Seychelles

veris:country="KZ"

Kazakhstan

veris:country="KY"

Cayman Islands

veris:country="SG"

Singapore

veris:country="SE"

Sweden

veris:country="SD"

Sudan

veris:country="DO"

Dominican Republic

veris:country="DM"

Dominica

veris:country="DJ"

Djibouti

veris:country="DK"

Denmark

veris:country="VG"

British Virgin Islands

veris:country="DE"

Germany

veris:country="YE"

Yemen

veris:country="Other"

Other

veris:country="DZ"

Algeria

veris:country="US"

United States of America

veris:country="UY"

Uruguay

veris:country="YT"

Mayotte

veris:country="UM"

United States Minor Outlying Islands

veris:country="LB"

Lebanon

veris:country="LC"

Saint Lucia

veris:country="LA"

Lao People’s Democratic Republic

veris:country="TV"

Tuvalu

veris:country="TW"

Taiwan, Province of China

veris:country="TT"

Trinidad and Tobago

veris:country="TR"

Turkey

veris:country="LK"

Sri Lanka

veris:country="LI"

Liechtenstein

veris:country="LV"

Latvia

veris:country="TO"

Tonga

veris:country="LT"

Lithuania

veris:country="LU"

Luxembourg

veris:country="LR"

Liberia

veris:country="LS"

Lesotho

veris:country="TH"

Thailand

veris:country="TF"

French Southern Territories

veris:country="TG"

Togo

veris:country="TD"

Chad

veris:country="TC"

Turks and Caicos Islands

veris:country="LY"

Libya

veris:country="VA"

Holy See

veris:country="VC"

Saint Vincent and the Grenadines

veris:country="AE"

United Arab Emirates

veris:country="AD"

Andorra

veris:country="AG"

Antigua and Barbuda

veris:country="AF"

Afghanistan

veris:country="AI"

Anguilla

veris:country="VI"

United States Virgin Islands

veris:country="IS"

Iceland

veris:country="IR"

Iran (Islamic Republic of)

veris:country="AM"

Armenia

veris:country="AL"

Albania

veris:country="AO"

Angola

veris:country="AQ"

Antarctica

veris:country="AS"

American Samoa

veris:country="AR"

Argentina

veris:country="AU"

Australia

veris:country="AT"

Austria

veris:country="AW"

Aruba

veris:country="IN"

India

veris:country="AX"

Aland Islands

veris:country="AZ"

Azerbaijan

veris:country="IE"

Ireland

veris:country="ID"

Indonesia

veris:country="UA"

Ukraine

veris:country="QA"

Qatar

veris:country="MZ"

Mozambique

impact:overall_rating

veris:impact:overall_rating="Insignificant"

Insignificant: Impact absorbed by normal activities

veris:impact:overall_rating="Catastrophic"

Catastrophic: A business-ending event (don’t choose this if the victim will continue operations)

veris:impact:overall_rating="Distracting"

Distracting: Limited "hard costs", but impact felt through having to deal with the incident rather than conducting normal duties

veris:impact:overall_rating="Damaging"

Damaging: Real and serious effect on the "bottom line" and/or long-term ability to generate revenue

veris:impact:overall_rating="Unknown"

Unknown

veris:impact:overall_rating="Painful"

Painful: Limited "hard costs", but impact felt through having to deal with the incident rather than conducting normal duties

actor:motive

veris:actor:motive="Grudge"

Grudge or personal offense

veris:actor:motive="Financial"

Financial or personal gain

veris:actor:motive="NA"

Not Applicable (unintentional action)

veris:actor:motive="Ideology"

Ideology or protest

veris:actor:motive="Convenience"

Convenience of expediency

veris:actor:motive="Other"

Other

veris:actor:motive="Unknown"

Unknown

veris:actor:motive="Fun"

Fun, curiosity, or pride

veris:actor:motive="Fear"

Fear or duress

veris:actor:motive="Espionage"

Espionage or competitive advantage

veris:actor:motive="Secondary"

Aid in a different attack

asset:management

veris:asset:management="NA"

Not applicable

veris:asset:management="Internal"

Internally managed

veris:asset:management="External"

Externally managed

veris:asset:management="Unknown"

Unknown

asset:variety

veris:asset:variety="M - Flash drive"

Media - Flash drive or card

veris:asset:variety="S - Print"

Server - Print

veris:asset:variety="P - Guard"

People - Guard

veris:asset:variety="S - Database"

Server - Database

veris:asset:variety="N - PBX"

Network - Private branch exchange (PBX)

veris:asset:variety="M - Other"

Media - Other/Unknown

veris:asset:variety="S - Other"

Server - Other/Unknown

veris:asset:variety="P - System admin"

People - Administrator

veris:asset:variety="S - POS controller"

Server - POS controller

veris:asset:variety="T - Other"

Public Terminal - Other/Unknown

veris:asset:variety="N - Camera"

Network - Camera or surveillance system

veris:asset:variety="S - Unknown"

Server - Unknown

veris:asset:variety="S - DHCP"

Server - DHCP

veris:asset:variety="U - POS terminal"

User Device - POS terminal

veris:asset:variety="N - LAN"

Network - Wired LAN

veris:asset:variety="P - Manager"

People - Manager

veris:asset:variety="M - Payment card"

Media - Payment card (e.g., magstripe, EMV)

veris:asset:variety="N - Public WAN"

Network - Public WAN

veris:asset:variety="P - Former employee"

People - Former employee

veris:asset:variety="S - Authentication"

Server - Authentication

veris:asset:variety="U - Mobile phone"

User Device - Mobile phone or smartphone

veris:asset:variety="N - Router or switch"

Network - Router or switch

veris:asset:variety="T - Kiosk"

Public Terminal - Self-service kiosk

veris:asset:variety="N - HSM"

Network - Hardware security module (HSM)

veris:asset:variety="U - Peripheral"

User Device - Peripheral (e.g., printer, copier, fax)

veris:asset:variety="S - Code repository"

Server - Code repository

veris:asset:variety="S - SCADA"

Server - SCADA system

veris:asset:variety="P - End-user"

People - End-user

veris:asset:variety="N - SAN"

Network - Storage area network (SAN)

veris:asset:variety="T - ATM"

Public Terminal - Automated Teller Machine (ATM)

veris:asset:variety="N - RTU"

Network - Remote terminal unit (RTU)

veris:asset:variety="Unknown"

Unknown

veris:asset:variety="M - Smart card"

Media - Identity smart card

veris:asset:variety="N - IDS"

Network - IDS or IPs

veris:asset:variety="N - PLC"

Network - Programmable logic controller (PLC)

veris:asset:variety="N - Other"

Network - Other/Unknown

veris:asset:variety="P - Cashier"

People - Cashier

veris:asset:variety="P - Executive"

People - Executive

veris:asset:variety="U - Desktop"

User Device - Desktop or workstation

veris:asset:variety="U - Tablet"

User Device - Tablet

veris:asset:variety="N - Firewall"

Network - Firewall

veris:asset:variety="P - Customer"

People - Customer

veris:asset:variety="S - Mainframe"

Server - Mainframe

veris:asset:variety="S - Directory"

Server - Directory (LDAP, AD)

veris:asset:variety="U - Auth token"

User Device - Authentication token or device

veris:asset:variety="U - Media"

User Device - Media player or recorder

veris:asset:variety="T - Gas terminal"

Public Terminal - Gas "pay-at-the-pump" terminal

veris:asset:variety="T - PED pad"

Public Terminal - Detached PIN pad or card reader

veris:asset:variety="M - Disk drive"

Media - Hard disk drive

veris:asset:variety="S - VM host"

Server - Virtual Host

veris:asset:variety="P - Auditor"

People - Auditor

veris:asset:variety="U - VoIP phone"

User Device - VoIP phone

veris:asset:variety="N - Broadband"

Network - Mobile broadband network

veris:asset:variety="U - Other"

User Device - Other/Unknown

veris:asset:variety="U - Telephone"

User Device - Telephone

veris:asset:variety="P - Call center"

People - Call center

veris:asset:variety="N - Private WAN"

Network - Private WAN

veris:asset:variety="S - DNS"

Server - DNS

veris:asset:variety="P - Helpdesk"

People - Helpdesk

veris:asset:variety="N - Telephone"

Network - Telephone

veris:asset:variety="U - Laptop"

User Device - Laptop

veris:asset:variety="S - Log"

Server - Log or event management

veris:asset:variety="P - Finance"

People - Finance

veris:asset:variety="P - Human resources"

People - Human resources

veris:asset:variety="N - VoIP adapter"

Network - VoIP adapter

veris:asset:variety="S - Backup"

Server - Backup

veris:asset:variety="P - Partner"

People - Partner

veris:asset:variety="P - Maintenance"

People - Maintenance

veris:asset:variety="S - Payment switch"

Server - Payment switch or gateway

veris:asset:variety="S - DCS"

Server - Distributed control system (DCS)

veris:asset:variety="P - Other"

People - Other/Unknown

veris:asset:variety="S - Proxy"

Server - Proxy

veris:asset:variety="S - Mail"

Server - Mail

veris:asset:variety="M - Tapes"

Media - Backup tapes

veris:asset:variety="S - Remote access"

Server - Remote access

veris:asset:variety="N - Access reader"

Network - Access control reader (e.g., badge, biometric)

veris:asset:variety="S - File"

Server - File

veris:asset:variety="S - Web application"

Server - Web application

veris:asset:variety="M - Documents"

Media - Documents

veris:asset:variety="N - WLAN"

Network - Wireless LAN

veris:asset:variety="P - Developer"

People - Developer

veris:asset:variety="M - Disk media"

Media - Disk media (e.g., CDs, DVDs)

asset:accessibility

veris:asset:accessibility="NA"

Not applicable

veris:asset:accessibility="Internal"

Internally accessible

veris:asset:accessibility="Unknown"

Unknown

veris:asset:accessibility="External"

Publicly accessible

veris:asset:accessibility="Isolated"

Internally isolated or restricted environment

asset:governance

veris:asset:governance="3rd party hosted"

Hosted by 3rd party

veris:asset:governance="Unknown"

Unknown

veris:asset:governance="3rd party managed"

Managed by 3rd party

veris:asset:governance="3rd party owned"

Owned by 3rd party

veris:asset:governance="Personally owned"

Personally owned asset

veris:asset:governance="Internally isolated"

Isolated internal asset

asset:hosting

veris:asset:hosting="External shared"

Externally hosted in a shared envirnoment

veris:asset:hosting="External dedicated"

Externally hosted in a dedicated envirnoment

veris:asset:hosting="NA"

Not applicable

veris:asset:hosting="Internal"

Internally hosted

veris:asset:hosting="External"

Externally hosted (unsure if dedicated or shared)

veris:asset:hosting="Unknown"

Unknown

asset:ownership

veris:asset:ownership="Customer"

Customer owned

veris:asset:ownership="Unknown"

Unknown

veris:asset:ownership="Victim"

Victim owned

veris:asset:ownership="NA"

Not applicable

veris:asset:ownership="Employee"

Employee owned

veris:asset:ownership="Partner"

Partner owned

asset:cloud

veris:asset:cloud="Hosting error"

Misconfiguration or error by hosting provider

veris:asset:cloud="User breakout"

Elevation of privilege by another customer in shared environment

veris:asset:cloud="Unknown"

Unknown

veris:asset:cloud="Other"

Other

veris:asset:cloud="Hosting governance"

Lack of security process or procedure by hosting provider

veris:asset:cloud="Customer attack"

Penetration of another web site on shared device

veris:asset:cloud="Hypervisor"

Hypervisor break-out attack

veris:asset:cloud="Partner application"

Application vulnerability in partner-developed application

victim:employee_count

veris:victim:employee_count="1001 to 10000"

1,001 to 10,000 employees

veris:victim:employee_count="Over 100000"

Over 100,0001 employees

veris:victim:employee_count="Large"

Large organizations (over 1,000 employees)

veris:victim:employee_count="Unknown"

Unknown number of employees

veris:victim:employee_count="50001 to 100000"

50,001 to 100,000 employees

veris:victim:employee_count="101 to 1000"

101 to 1,000 employees

veris:victim:employee_count="25001 to 50000"

25,001 to 50,000 employees

veris:victim:employee_count="10001 to 25000"

10,001 to 25,000 employees

veris:victim:employee_count="Small"

Small organizations (1,000 employees or less)

veris:victim:employee_count="1 to 10"

1 to 10 employees

veris:victim:employee_count="11 to 100"

11 to 100 employees

timeline:unit

veris:timeline:unit="Months"

Months

veris:timeline:unit="Seconds"

Seconds

veris:timeline:unit="NA"

NA

veris:timeline:unit="Never"

Never

veris:timeline:unit="Days"

Days

veris:timeline:unit="Years"

Years

veris:timeline:unit="Hours"

Hours

veris:timeline:unit="Unknown"

Unknown

veris:timeline:unit="Weeks"

Weeks

veris:timeline:unit="Minutes"

Minutes

impact:loss:rating

veris:impact:loss:rating="Unknown"

Unknown

veris:impact:loss:rating="Major"

Major

veris:impact:loss:rating="Moderate"

Moderate

veris:impact:loss:rating="None"

None

veris:impact:loss:rating="Minor"

Minor

impact:loss:variety

veris:impact:loss:variety="Legal and regulatory"

Legal and regulatory costs

veris:impact:loss:variety="Asset and fraud"

Asset and fraud-related losses

veris:impact:loss:variety="Business disruption"

Business disruption

veris:impact:loss:variety="Response and recovery"

Response and recovery costs

veris:impact:loss:variety="Competitive advantage"

Loss of competitive advantage

veris:impact:loss:variety="Operating costs"

Increased operating costs

veris:impact:loss:variety="Brand damage"

Brand and market damage

attribute:integrity:variety

veris:attribute:integrity:variety="Misrepresentation"

Misrepresentation

veris:attribute:integrity:variety="Modify data"

Modified stored data or content

veris:attribute:integrity:variety="Unknown"

Unknown

veris:attribute:integrity:variety="Created account"

Created new user account

veris:attribute:integrity:variety="Defacement"

Deface content

veris:attribute:integrity:variety="Log tampering"

Log tampering or modification

veris:attribute:integrity:variety="Modify privileges"

Modified privileges or permissions

veris:attribute:integrity:variety="Software installation"

Software installation or code modification

veris:attribute:integrity:variety="Other"

Other

veris:attribute:integrity:variety="Fraudulent transaction"

Initiate fraudulent transaction

veris:attribute:integrity:variety="Alter behavior"

Influence or alter human behavior

veris:attribute:integrity:variety="Hardware tampering"

Hardware tampering or physical alteration

veris:attribute:integrity:variety="Modify configuration"

Modified configuration or services

veris:attribute:integrity:variety="Repurpose"

Repurposed asset for unauthorized function

attribute:availability:variety

veris:attribute:availability:variety="Acceleration"

Acceleration

veris:attribute:availability:variety="Interruption"

Interruption

veris:attribute:availability:variety="Loss"

Loss

veris:attribute:availability:variety="Unknown"

Unknown

veris:attribute:availability:variety="Degradation"

Performance degradation

veris:attribute:availability:variety="Other"

Other

veris:attribute:availability:variety="Obscuration"

Conversion or obscuration

veris:attribute:availability:variety="Destruction"

Destruction

attribute:confidentiality:data_victim

veris:attribute:confidentiality:data_victim="Customer"

Customer

veris:attribute:confidentiality:data_victim="Patient"

Patient

veris:attribute:confidentiality:data_victim="Unknown"

Unknown

veris:attribute:confidentiality:data_victim="Other"

Other

veris:attribute:confidentiality:data_victim="Student"

Student

veris:attribute:confidentiality:data_victim="Employee"

Employee

veris:attribute:confidentiality:data_victim="Partner"

Partner

attribute:confidentiality:state

veris:attribute:confidentiality:state="Unknown"

Unknown

veris:attribute:confidentiality:state="Transmitted encrypted"

Transmitted encrypted

veris:attribute:confidentiality:state="Transmitted unencrypted"

Transmitted unencrypted

veris:attribute:confidentiality:state="Stored"

Stored

veris:attribute:confidentiality:state="Transmitted"

Transmitted

veris:attribute:confidentiality:state="Processed"

Processed

veris:attribute:confidentiality:state="Stored encrypted"

Stored encrypted

veris:attribute:confidentiality:state="Stored unencrypted"

Stored unencrypted

attribute:confidentiality:data_disclosure

veris:attribute:confidentiality:data_disclosure="Unknown"

Unknown

veris:attribute:confidentiality:data_disclosure="Yes"

Yes (confirmed)

veris:attribute:confidentiality:data_disclosure="Potentially"

Potentially (at risk)

veris:attribute:confidentiality:data_disclosure="No"

No

actor:internal:job_change

veris:actor:internal:job_change="Lateral move"

Lateral move

veris:actor:internal:job_change="Job eval"

Recent poor job evaluation

veris:actor:internal:job_change="Unknown"

Unknown

veris:actor:internal:job_change="Personal issues"

Personal issues

veris:actor:internal:job_change="Let go"

Fired, laid off, or let go

veris:actor:internal:job_change="Reprimanded"

Recently reprimanded

veris:actor:internal:job_change="Hired"

Recently hired

veris:actor:internal:job_change="Passed over"

Recently passed over for promotion

veris:actor:internal:job_change="Demoted"

Recently demoted or hours reduced

veris:actor:internal:job_change="Promoted"

Recently promoted

veris:actor:internal:job_change="Resigned"

Recently resigned

veris:actor:internal:job_change="Other"

Other

actor:internal:variety

veris:actor:internal:variety="End-user"

End-user or regular employee

veris:actor:internal:variety="Human resources"

Human resources staff

veris:actor:internal:variety="Finance"

Finance or accounting staff

veris:actor:internal:variety="Unknown"

Unknown

veris:actor:internal:variety="Helpdesk"

Helpdesk staff

veris:actor:internal:variety="Executive"

Executive or upper management

veris:actor:internal:variety="Cashier"

Cashier, teller, or waiter

veris:actor:internal:variety="Manager"

Manager or supervisor

veris:actor:internal:variety="Guard"

Security guard

veris:actor:internal:variety="Other"

Other

veris:actor:internal:variety="Auditor"

Auditor

veris:actor:internal:variety="Maintenance"

Maintenance or janitorial staff

veris:actor:internal:variety="Call center"

Call center staff

veris:actor:internal:variety="System admin"

System or network administrator

veris:actor:internal:variety="Developer"

Software developer

actor:external:variety

veris:actor:external:variety="Customer"

Customer (B2C)

veris:actor:external:variety="Organized crime"

Organized or professional criminal group

veris:actor:external:variety="Acquaintance"

Relative or acquaintance of employee

veris:actor:external:variety="Competitor"

Competitor

veris:actor:external:variety="Unaffiliated"

Unaffiliated person(s)

veris:actor:external:variety="Force majeure"

Force majeure (nature and chance)

veris:actor:external:variety="Former employee"

Former employee (no longer had access)

veris:actor:external:variety="Nation-state"

Nation-state

veris:actor:external:variety="Activist"

Activist group

veris:actor:external:variety="Terrorist"

Terrorist group

veris:actor:external:variety="Auditor"

Auditor

veris:actor:external:variety="Unknown"

Unknown

veris:actor:external:variety="State-affiliated"

State-sponsored or affiliated group

veris:actor:external:variety="Other"

Other

action:malware:vector

veris:action:malware:vector="Remote injection"

Remotely injected by agent (i.e. via SQLi)

veris:action:malware:vector="Software update"

Included in automated software update

veris:action:malware:vector="Instant messaging"

Instant Messaging

veris:action:malware:vector="Email attachment"

Email via user-executed attachment

veris:action:malware:vector="Direct install"

Directly installed or inserted by threat agent (after system access)

veris:action:malware:vector="Download by malware"

Downloaded and installed by local malware

veris:action:malware:vector="Removable media"

Removable storage media or devices

veris:action:malware:vector="Web drive-by"

Web via auto-executed or "drive-by" infection

veris:action:malware:vector="Email link"

Email via embedded link

veris:action:malware:vector="Network propagation"

Network propagation

veris:action:malware:vector="Unknown"

Unknown

veris:action:malware:vector="Email autoexecute"

Email via automatic execution

veris:action:malware:vector="Web download"

Web via user-executed or downloaded content

veris:action:malware:vector="Other"

Other

action:malware:variety

veris:action:malware:variety="Spam"

Send spam

veris:action:malware:variety="Unknown"

Unknown

veris:action:malware:variety="Packet sniffer"

Packet sniffer (capture data from network)

veris:action:malware:variety="Backdoor"

Backdoor (enable remote access)

veris:action:malware:variety="Exploit vuln"

Exploit vulnerability in code (vs misconfig or weakness)

veris:action:malware:variety="Other"

Other

veris:action:malware:variety="Password dumper"

Password dumper (extract credential hashes)

veris:action:malware:variety="Scan network"

Scan or footprint network

veris:action:malware:variety="Downloader"

Downloader (pull updates or other malware)

veris:action:malware:variety="Adminware"

System or network utilities (e.g., PsTools, Netcat)

veris:action:malware:variety="Click fraud"

Click fraud or Bitcoin mining

veris:action:malware:variety="Adware"

Adware

veris:action:malware:variety="C2"

Command and control (C2)

veris:action:malware:variety="Worm"

Worm (propagate to other systems or devices)

veris:action:malware:variety="Spyware/Keylogger"

Spyware, keylogger or form-grabber (capture user input or activity)

veris:action:malware:variety="Brute force"

Brute force attack

veris:action:malware:variety="Capture app data"

Capture data from application or system process

veris:action:malware:variety="Ram scraper"

Ram scraper or memory parser (capture data from volatile memory)

veris:action:malware:variety="Disable controls"

Disable or interfere with security controls

veris:action:malware:variety="Capture stored data"

Capture data stored on system disk

veris:action:malware:variety="Ransomware"

Ransomware (encrypt or seize stored data)

veris:action:malware:variety="Export data"

Export data to another site or system

veris:action:malware:variety="Client-side attack"

Client-side or browser attack (e.g., redirection, XSS, MitB)

veris:action:malware:variety="SQL injection"

SQL injection attack

veris:action:malware:variety="Rootkit"

Rootkit (maintain local privileges and stealth)

veris:action:malware:variety="Destroy data"

Destroy or corrupt stored data

veris:action:malware:variety="DoS"

DoS attack

action:social:vector

veris:action:social:vector="In-person"

In-person

veris:action:social:vector="Social media"

Social media or networking

veris:action:social:vector="Documents"

Documents

veris:action:social:vector="Unknown"

Unknown

veris:action:social:vector="SMS"

SMS or texting

veris:action:social:vector="Phone"

Phone

veris:action:social:vector="Website"

Website

veris:action:social:vector="Other"

Other

veris:action:social:vector="IM"

Instant messaging

veris:action:social:vector="Removable media"

Removable storage media

veris:action:social:vector="Email"

Email

veris:action:social:vector="Software"

Software

action:social:target

veris:action:social:target="Customer"

Customer (B2C)

veris:action:social:target="End-user"

End-user or regular employee

veris:action:social:target="Human resources"

Human resources staff

veris:action:social:target="Finance"

Finance or accounting staff

veris:action:social:target="Unknown"

Unknown

veris:action:social:target="Helpdesk"

Helpdesk staff

veris:action:social:target="Executive"

Executive or upper management

veris:action:social:target="Cashier"

Cashier, teller or waiter

veris:action:social:target="Manager"

Manager or supervisor

veris:action:social:target="Former employee"

Former employee

veris:action:social:target="Guard"

Security guard

veris:action:social:target="Other"

Other

veris:action:social:target="Auditor"

Auditor

veris:action:social:target="Maintenance"

Maintenance or janitorial staff

veris:action:social:target="Call center"

Call center staff

veris:action:social:target="Partner"

Partner (B2B)

veris:action:social:target="System admin"

System or network administrator

veris:action:social:target="Developer"

Software developer

action:social:variety

veris:action:social:variety="Scam"

Online scam or hoax (e.g., scareware, 419 scam, auction fraud)

veris:action:social:variety="Phishing"

Phishing (or any type of *ishing)

veris:action:social:variety="Elicitation"

Elicitation (subtle extraction of info through conversation)

veris:action:social:variety="Unknown"

Unknown

veris:action:social:variety="Spam"

Spam (unsolicited or undesired email and advertisements)

veris:action:social:variety="Influence"

Influence tactics (Leveraging authority or obligation, framing, etc)

veris:action:social:variety="Propaganda"

Propaganda or disinformation

veris:action:social:variety="Forgery"

Forgery or counterfeiting (fake hardware, software, documents, etc)

veris:action:social:variety="Bribery"

Bribery or solicitation

veris:action:social:variety="Other"

Other

veris:action:social:variety="Pretexting"

Pretexting (dialogue leveraging invented scenario)

veris:action:social:variety="Extortion"

Extortion or blackmail

veris:action:social:variety="Baiting"

Baiting (planting infected media)

action:environmental:variety

veris:action:environmental:variety="Hazmat"

Hazardous material

veris:action:environmental:variety="Temperature"

Extreme temperature

veris:action:environmental:variety="Unknown"

Unknown

veris:action:environmental:variety="Hurricane"

Hurricane

veris:action:environmental:variety="Ice"

Ice and snow

veris:action:environmental:variety="Meteorite"

Meteorite

veris:action:environmental:variety="Other"

Other

veris:action:environmental:variety="Pathogen"

Pathogen

veris:action:environmental:variety="Landslide"

Landslide

veris:action:environmental:variety="Tornado"

Tornado

veris:action:environmental:variety="Leak"

Water leak

veris:action:environmental:variety="Earthquake"

Earthquake

veris:action:environmental:variety="Particulates"

Particulate matter (e.g., dust, smoke)

veris:action:environmental:variety="Power failure"

Power failure or fluctuation

veris:action:environmental:variety="EMI"

Electromagnetic interference (EMI)

veris:action:environmental:variety="Humidity"

Humidity

veris:action:environmental:variety="Tsunami"

Tsunami

veris:action:environmental:variety="ESD"

Electrostatic discharge (ESD)

veris:action:environmental:variety="Deterioration"

Deterioration and degradation

veris:action:environmental:variety="Volcano"

Volcanic eruption

veris:action:environmental:variety="Lightning"

Lightning

veris:action:environmental:variety="Wind"

Wind

veris:action:environmental:variety="Flood"

Flood

veris:action:environmental:variety="Vermin"

Vermin

veris:action:environmental:variety="Fire"

Fire

action:error:vector

veris:action:error:vector="Random error"

Random error (no reason, no fault)

veris:action:error:vector="Carelessness"

Carelessness

veris:action:error:vector="Other"

Other

veris:action:error:vector="Unknown"

Unknown

veris:action:error:vector="Inadequate processes"

Inadequate or insufficient processes

veris:action:error:vector="Inadequate technology"

Inadequate or insufficient technology resources

veris:action:error:vector="Inadequate personnel"

Inadequate or insufficient personnel

action:error:variety

veris:action:error:variety="Disposal error"

Disposal error

veris:action:error:variety="Omission"

Omission (something intended, but not done)

veris:action:error:variety="Loss"

Loss or misplacement

veris:action:error:variety="Unknown"

Unknown

veris:action:error:variety="Maintenance error"

Maintenance error

veris:action:error:variety="Misinformation"

Misinformation (unintentionally giving false info)

veris:action:error:variety="Physical accidents"

Physical accidents (e.g., drops, bumps, spills)

veris:action:error:variety="Publishing error"

Publishing error (private info to public doc or site)

veris:action:error:variety="Malfunction"

Technical malfunction or glitch

veris:action:error:variety="Capacity shortage"

Poor capacity planning

veris:action:error:variety="Other"

Other

veris:action:error:variety="Programming error"

Programming error (flaws or bugs in custom code)

veris:action:error:variety="Data entry error"

Data entry error

veris:action:error:variety="Gaffe"

Gaffe (social or verbal slip)

veris:action:error:variety="Misconfiguration"

Misconfiguration

veris:action:error:variety="Misdelivery"

Misdelivery (send wrong info or to wrong recipient)

veris:action:error:variety="Classification error"

Classification or labeling error

action:misuse:vector

veris:action:misuse:vector="Physical access"

Physical access within corporate facility

veris:action:misuse:vector="Remote access"

Remote access connection to corporate network (i.e. VPN)

veris:action:misuse:vector="LAN access"

Local network access within corporate facility

veris:action:misuse:vector="Unknown"

Unknown

veris:action:misuse:vector="Non-corporate"

Non-corporate facilities or networks

veris:action:misuse:vector="Other"

Other

action:misuse:variety

veris:action:misuse:variety="Unapproved software"

Use of unapproved software or services

veris:action:misuse:variety="Illicit content"

Storage or distribution of illicit content

veris:action:misuse:variety="Unapproved workaround"

Unapproved workaround or shortcut

veris:action:misuse:variety="Unapproved hardware"

Use of unapproved hardware or devices

veris:action:misuse:variety="Unknown"

Unknown

veris:action:misuse:variety="Email misuse"

Inappropriate use of email or IM

veris:action:misuse:variety="Possession abuse"

Abuse of physical access to asset

veris:action:misuse:variety="Other"

```
Other
```

veris:action:misuse:variety="Net misuse"

Inappropriate use of network or Web access

veris:action:misuse:variety="Data mishandling"

Handling of data in an unapproved manner

veris:action:misuse:variety="Privilege abuse"

Abuse of system access privileges

veris:action:misuse:variety="Knowledge abuse"

Abuse of private or entrusted knowledge

action:hacking:vector

veris:action:hacking:vector="Physical access"

Physical access or connection (i.e., at keyboard or via cable)

veris:action:hacking:vector="Command shell"

Remote shell

veris:action:hacking:vector="Unknown"

Unknown

veris:action:hacking:vector="Backdoor or C2"

Backdoor or command and control channel

veris:action:hacking:vector="Web application"

Web application

veris:action:hacking:vector="Desktop sharing"

Graphical desktop sharing (RDP, VNC, PCAnywhere, Citrix)

veris:action:hacking:vector="3rd party desktop"

3rd party online desktop sharing (LogMeIn, Go2Assist)

veris:action:hacking:vector="Partner"

Partner connection or credential

veris:action:hacking:vector="VPN"

VPN

veris:action:hacking:vector="Other"

Other

action:hacking:variety

veris:action:hacking:variety="XSS"

Cross-site scripting

veris:action:hacking:variety="HTTP Response Splitting"

HTTP Response Splitting

veris:action:hacking:variety="Unknown"

Unknown

veris:action:hacking:variety="Buffer overflow"

Buffer overflow

veris:action:hacking:variety="Format string attack"

Format string attack

veris:action:hacking:variety="LDAP injection"

LDAP injection

veris:action:hacking:variety="SSI injection"

SSI injection

veris:action:hacking:variety="MitM"

Man-in-the-middle attack

veris:action:hacking:variety="Path traversal"

Path traversal

veris:action:hacking:variety="URL redirector abuse"

URL redirector abuse

veris:action:hacking:variety="Use of backdoor or C2"

Use of Backdoor or C2 channel

veris:action:hacking:variety="Mail command injection"

Mail command injection

veris:action:hacking:variety="Virtual machine escape"

Virtual machine escape

veris:action:hacking:variety="OS commanding"

OS commanding

veris:action:hacking:variety="Soap array abuse"

Soap array abuse

veris:action:hacking:variety="Footprinting"

Footprinting and fingerprinting

veris:action:hacking:variety="Cryptanalysis"

Cryptanalysis

veris:action:hacking:variety="SQLi"

SQL injection

veris:action:hacking:variety="XML external entities"

XML external entities

veris:action:hacking:variety="Abuse of functionality"

Abuse of functionality

veris:action:hacking:variety="XML injection"

XML injection

veris:action:hacking:variety="Routing detour"

Routing detour

veris:action:hacking:variety="HTTP response smuggling"

HTTP response smuggling

veris:action:hacking:variety="Forced browsing"

Forced browsing or predictable resource location

veris:action:hacking:variety="Cache poisoning"

Cache poisoning

veris:action:hacking:variety="Null byte injection"

Null byte injection

veris:action:hacking:variety="Reverse engineering"

Reverse engineering

veris:action:hacking:variety="Brute force"

Brute force or password guessing attacks

veris:action:hacking:variety="Fuzz testing"

Fuzz testing

veris:action:hacking:variety="Offline cracking"

Offline password or key cracking (e.g., rainbow tables, Hashcat, JtR)

veris:action:hacking:variety="CSRF"

Cross-site request forgery

veris:action:hacking:variety="XML entity expansion"

XML entity expansion

veris:action:hacking:variety="RFI"

Remote file inclusion

veris:action:hacking:variety="Session fixation"

Session fixation

veris:action:hacking:variety="Integer overflows"

Integer overflows

veris:action:hacking:variety="XQuery injection"

XQuery injection

veris:action:hacking:variety="Pass-the-hash"

Pass-the-hash

veris:action:hacking:variety="XML attribute blowup"

XML attribute blowup

veris:action:hacking:variety="Session prediction"

Credential or session prediction

veris:action:hacking:variety="Use of stolen creds"

Use of stolen authentication credentials

veris:action:hacking:variety="HTTP request smuggling"

HTTP request smuggling

veris:action:hacking:variety="XPath injection"

XPath injection

veris:action:hacking:variety="Other"

Other

veris:action:hacking:variety="DoS"

Denial of service

veris:action:hacking:variety="Special element injection"

Special element injection

veris:action:hacking:variety="HTTP request splitting"

HTTP request splitting

veris:action:hacking:variety="Session replay"

Session replay

action:physical:vector

veris:action:physical:vector="Personal vehicle"

Personal vehicle

veris:action:physical:vector="Visitor privileges"

Given temporary visitor access

veris:action:physical:vector="Public facility"

Public facility or area

veris:action:physical:vector="Victim grounds"

Victim outdoor grounds

veris:action:physical:vector="Uncontrolled location"

The location was uncontrolled (public)

veris:action:physical:vector="Partner vehicle"

Partner vehicle (e.g., delivery truck)

veris:action:physical:vector="Victim work area"

Victim private or work area (e.g., office space)

veris:action:physical:vector="Victim secure area"

Victim high security area (e.g., server room, R&D labs)

veris:action:physical:vector="Partner facility"

Partner facility or area

veris:action:physical:vector="Personal residence"

Personal residence

veris:action:physical:vector="Other"

Other

veris:action:physical:vector="Public vehicle"

Public vehicle (e.g., plane, taxi)

veris:action:physical:vector="Unknown"

Unknown

veris:action:physical:vector="Victim public area"

Victim public or customer area (e.g., lobby, storefront)

veris:action:physical:vector="Privileged access"

Held privileged access to location

action:physical:variety

veris:action:physical:variety="Skimmer"

Installing card skimming device

veris:action:physical:variety="Snooping"

Snooping (sneak about to gain info or access)

veris:action:physical:variety="Tampering"

Tampering (alter physical form or function)

veris:action:physical:variety="Unknown"

Unknown

veris:action:physical:variety="Theft"

Theft (taking assets without permission)

veris:action:physical:variety="Connection"

Connection

veris:action:physical:variety="Surveillance"

Surveillance (monitoring and observation)

veris:action:physical:variety="Assault"

Assault (threats or acts of physical violence)

veris:action:physical:variety="Other"

Other

veris:action:physical:variety="Wiretapping"

Wiretapping (Physical tap to comms line)

veris:action:physical:variety="Bypassed controls"

Bypassed physical barriers or controls

veris:action:physical:variety="Disabled controls"

Disabled physical barriers or controls

veris:action:physical:variety="Destruction"

Destruction (deliberate damaging or disabling)

attribute:confidentiality:data:variety

veris:attribute:confidentiality:data:variety="Source code"

Source code

veris:attribute:confidentiality:data:variety="Personal"

Personal or identifying information (e.g., addr, ID#, credit score)

veris:attribute:confidentiality:data:variety="Unknown"

Unknown

veris:attribute:confidentiality:data:variety="Medical"

Medical records

veris:attribute:confidentiality:data:variety="Classified"

Classified information

veris:attribute:confidentiality:data:variety="System"

System information (e.g., config info, open services)

veris:attribute:confidentiality:data:variety="Digital certificate"

Digital certificate

veris:attribute:confidentiality:data:variety="Secrets"

Trade secrets

veris:attribute:confidentiality:data:variety="Internal"

Sensitive internal data (e.g., plans, reports, emails)

veris:attribute:confidentiality:data:variety="Virtual currency"

Virtual currency

veris:attribute:confidentiality:data:variety="Copyrighted"

Copyrighted material

veris:attribute:confidentiality:data:variety="Credentials"

Authentication credentials (e.g., pwds, OTPs, biometrics)

veris:attribute:confidentiality:data:variety="Other"

Other

veris:attribute:confidentiality:data:variety="Payment"

Payment card data (e.g., PAN, PIN, CVV2, Expiration)

veris:attribute:confidentiality:data:variety="Bank"

Bank account data

vocabulaire-des-probabilites-estimatives

vocabulaire-des-probabilites-estimatives namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Ce vocabulaire attribue des valeurs en pourcentage à certains énoncés de probabilité

degré-de-probabilité

Le tableau suivant attribue des valeurs en pourcentage à certains énoncés de probabilité. Les pourcentages sont tirés de l'ouvrage de Sherman Kent intitulé « Words of Estimative Probability » publié par le Centre for the Study of Intelligence de la CIA en 1964. 0% exprime une impossibilité et 100% exprime une certitude.

vocabulaire-des-probabilites-estimatives:degré-de-probabilité="presque-aucune-chance"

Presque aucune chance - Quasi impossible Presque impossible Minces chances Très douteux Très peu probable Très improbable Improbable Peu de chances - 7 % (marge d'erreur d'environ 5 %)

vocabulaire-des-probabilites-estimatives:degré-de-probabilité="probablement-pas"

Probablement pas - Invraisemblable Peu probable - 30 % (marge d'erreur d'environ 10 %)

vocabulaire-des-probabilites-estimatives:degré-de-probabilité="chances-à-peu-près-egales"

Chances à peu près égales - une chance sur deux - 50% (marge d'erreur d'environ 10 %)

vocabulaire-des-probabilites-estimatives:degré-de-probabilité="probable"

Probable - Vraisemblable Probable - 75 % (marge d'erreur d'environ 12 %)

vocabulaire-des-probabilites-estimatives:degré-de-probabilité="quasi-certaine"

Quasi certaine - Certain Presque certain Très probable - 93% (marge d’erreur d’environ 6 %)

workflow

workflow namespace available in JSON format at **this location**. The JSON format can be freely reused in your application or automatically enabled in MISP taxonomy.

Workflow support language is a common language to support intelligence analysts to perform their analysis on data and information.

todo

Todo are the actions to be performed by one or more analyst(s) to apply cognitive methods, evaluation(s), weightening information, to validate hypothesis or complete additional tasks to improve the overall information or data being tagged with a todo.

workflow:todo="expansion"

Expansion need to be applied to expand the information tagged

workflow:todo="review"

Additional review is required to reach a certain level of validation of the information tagged

workflow:todo="review-before-publication"

Review is required before publishing the information tagged

workflow:todo="review-for-false-positive"

Review the the information tagged to limit the number of false-positives and potentially remove any IDS/automation flag to avoid automation of the false-positives

workflow:todo="review-the-source-credibility"

Review the source credibility and add the corresponding marking like admiralty-scale on the origin

workflow:todo="create-missing-misp-galaxy-cluster-values"

Add potential MISP galaxy cluster values missing about the information tagged

workflow:todo="create-missing-misp-galaxy-cluster"

Create missing MISP galaxy cluster about the information tagged

workflow:todo="create-missing-misp-galaxy"

Create missing MISP galaxy at large about the information tagged (e.g. a new category of malware or activity)

workflow:todo="add-context"

Add contextual information about the information tagged

workflow:todo="add-tagging"

Add adequate tagging and classification about the information tagged

workflow:todo="check-passive-dns-for-shared-hosting"

Check Passive DNS (or similar techniques) to review if the information tagged is used within shared hosting

workflow:todo="review-classification"

Review the classification of the information tagged to ensure adequate marking of the information before publication

workflow:todo="review-the-grammar"

Review the grammar of the information tagged to improve the overall quality

state

State are the different states of the information or data being tagged.

workflow:state="incomplete"

Incomplete means that the information tagged is incomplete and has potential to be completed by other analysts, technical processes or the current analysts performing the analysis

workflow:state="complete"

Complete means that the information tagged reach a state of completeness with the current capabilities of the analyst

Mapping of taxonomies

Analysts relying on taxonomies don't always know the appropriate namespace to use but know which value to use for classification. The MISP mapping taxonomy allows to map a single classification into a series of machine-tag synonyms.

Table 1. Mapping table - **Adware**

Adware
veris:action:malware:variety="Adware"
malware_classification:malware-category="Adware"
ms-caro-malware:malware-type="Adware"

Table 2. Mapping table - **Brute Force**

Brute Force
ecsirt:intrusion-attempts="brute-force"
veris:action:malware:variety="Brute force"
europol-event:brute-force-attempt
enisa:nefarious-activity-abuse="brute-force"

Table 3. Mapping table - **DDoS**

DDoS
ecsirt:availability="ddos"
europol-incident:availability="dos-ddos"
ms-caro-malware:malware-type="DDoS"
circl:incident-classification="denial-of-service"
enisa:nefarious-activity-abuse="denial-of-service"

Table 4. Mapping table - **Downloader**

Downloader
veris:action:malware:variety="Downloader"
malware_classification:malware-category="Downloader"

Table 5. Mapping table - **Remote Access Tool**

Remote Access Tool
enisa:nefarious-activity-abuse="remote-access-tool"
ms-caro-malware:malware-type="RemoteAccess"

Table 6. Mapping table - **SQLi**

SQLi
circl:incident-classification="sql-injection"

veris:action:malware:variety="SQL injection"
veris:action:hacking:variety="SQLi"
enisa:nefarious-activity-abuse="web-application-attacks-injection-attacks-code-injection-SQL-XSS"
europol-event:sql-injection

Table 7. Mapping table - **Spyware**

Spyware
veris:action:malware:variety="Spyware/Keylogger"
malware_classification:malware-category="Spyware"
ms-caro-malware:malware-type="Spyware"
enisa:nefarious-activity-abuse="spyware-or-deceptive-adware"

Table 8. Mapping table - **Trojan**

Trojan
malware_classification:malware-category="Trojan"
ms-caro-malware:malware-type="Trojan"
ecsirt:malicious-code="trojan"

Table 9. Mapping table - **Virus**

Virus
malware_classification:malware-category="Virus"
ms-caro-malware:malware-type="Virus"
ecsirt:malicious-code="virus"

Table 10. Mapping table - **Worm**

Worm
veris:action:malware:variety="Worm"
malware_classification:malware-category="Worm"
ms-caro-malware:malware-type="Worm"
ecsirt:malicious-code="worm"

Table 11. Mapping table - **backdoor**

backdoor
ecsirt:intrusions="backdoor"
veris:action:malware:variety="Backdoor"
ms-caro-malware:malware-type="Backdoor"

Table 12. Mapping table - **brute force**

brute force
ecsirt:intrusion-attempts="brute-force"

veris:action:malware:variety="Brute force"
europol-event:brute-force-attempt
enisa:nefarious-activity-abuse="brute-force"

Table 13. Mapping table - **c&c**

c&c
ecsirt:malicious-code="c&c"
europol-incident:malware="c&c"
europol-event:c&c-server-hosting
veris:action:malware:variety="C2"

Table 14. Mapping table - **exploit**

exploit
veris:action:malware:variety="Exploit vuln"
ecsirt:intrusion-attempts="exploit"
europol-event:exploit
europol-incident:intrusion="exploitation-vulnerability"
ms-caro-malware:malware-type="Exploit"

Table 15. Mapping table - **malware**

malware
ecsirt:malicious-code="malware"
circl:incident-classification="malware"

Table 16. Mapping table - **phishing**

phishing
circl:incident-classification="phishing"
ecsirt:fraud="phishing"
veris:action:social:variety="Phishing"
europol-incident:information-gathering="phishing"
enisa:nefarious-activity-abuse="phishing-attacks"

Table 17. Mapping table - **ransomware**

ransomware
ecsirt:malicious-code="ransomware"
enisa:nefarious-activity-abuse="ransomware"
malware_classification:malware-category="Ransomware"
ms-caro-malware:malware-type="Ransom"
veris:action:malware:variety="Ransomware"

Table 18. Mapping table - **rootkit**

rootkit
veris:action:malware:variety="Rootkit"
enisa:nefarious-activity-abuse="rootkits"
malware_classification:malware-category="Rootkit"

Table 19. Mapping table - **scan**

scan
circl:incident-classification="scan"
ecsirt:information-gathering="scanner"
europol-incident:information-gathering="scanning"

Table 20. Mapping table - **scan network**

scan network
veris:action:malware:variety="Scan network"
europol-event:network-scanning

Table 21. Mapping table - **spam**

spam
circl:incident-classification="spam"
ecsirt:abusive-content="spam"
enisa:nefarious-activity-abuse="spam"
europol-event:spam
europol-incident:abusive-content="spam"
veris:action:malware:variety="Spam"
veris:action:social:variety="Spam"

Table 22. Mapping table - **tlp-amber**

tlp-amber
tlp:amber
iep:traffic-light-protocol="AMBER"

Table 23. Mapping table - **tlp-green**

tlp-green
tlp:green
iep:traffic-light-protocol="GREEN"

Table 24. Mapping table - **tlp-red**

tlp-red
tlp:red

iep:traffic-light-protocol="RED"

Table 25. Mapping table - **tlp-white**

tlp-white
tlp:white
iep:traffic-light-protocol="WHITE"

Table 26. Mapping table - **xss**

xss
circl:incident-classification="XSS"
europol-event:xss