Emerging Threats Intelligence Features and Usage

Windows User

Registration

New users of ET Intelligence Query will need to register for an account at https://etadmin.proofpoint.com. The user will need to supply Proofpoint Emerging Threats with basic information to complete the registration process. The user will be given the option of creating, or joining a current organization. If the user is joining a current organization, approval by that organization's portal admin must be obtained. The user will be asked to verify the email address supplied, and will be granted approval by the organization admin if necessary.

Once registered and approved the user will have access to the ET Intelligence Query button on the toolbar of the portal landing page.
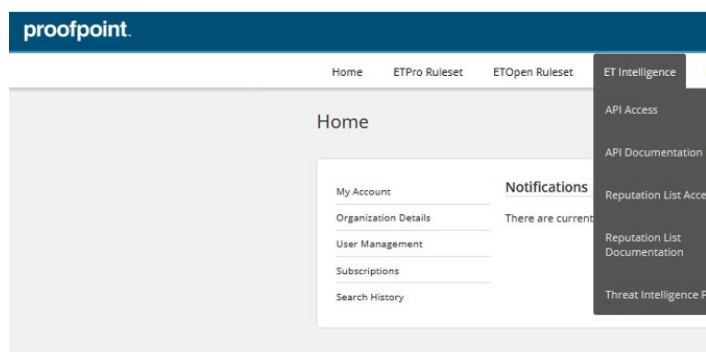

Figure 1: ET Intelligence Query Button

The user will be presented with "API Access and Search Options." Clicking the API Access hyperlink will present the user with their API authorization key. ET Intelligence Query API functionality is not the focus of this document. API documentation can be found at the link below:

https://apidocs.emergingthreats.net/#introduction

The search portal has been updated to https://threatintel.proofpoint.com which features a redesigned user interface. You will automatically be redirected to this site or can access it directly using your ET credentials.

Information Search

The ET Threat Intelligence Portal provides you with a powerful mechanism to search for different object types which you may have observed in your environment. Currently we offer five different searches in the search box.

1. IP Address: Simply enter the host IP address that you would like to search for in the search box. For example, 114.112.255.81

2. Domain: This would be the fully qualified domain name that you would like to evaluate the reputation of. Note that this is not a URL, but instead the base FQDN. For example, ilo.brenz.pl

3. Signature ID: Also known as SID, which is a term used for a rule identifier in Suricata and Snort. You can search for any ETPro or ET Open signature. For example, 2804682

4. SID Message Text: You can look for any text in the SID's to find any associated rules. This is an autocomplete function, so you can simply type any matching keywords to find. For example, "Angler".

5. MD5 Hash: This would be the MD5 for any sample which has been uploaded into the SensorNet/SandNet. Simply enter the MD5 hash for that sample: For example, 757782d6a88684b923aabbba62157205

6. SHA256 Hash: This would be the SHA256 for any sample which has been uploaded into the SensorNet/SandNet. Simply enter the SHA256 hash for that sample: For example, 040bc6452ce4671032622ca4b1a602f3ab8fdcc63f953b01567db028db8677ae

Note that if you click upon the text box, a pop up will appear which lets you click on sample entries. So you can immediately look at entries which change over time.
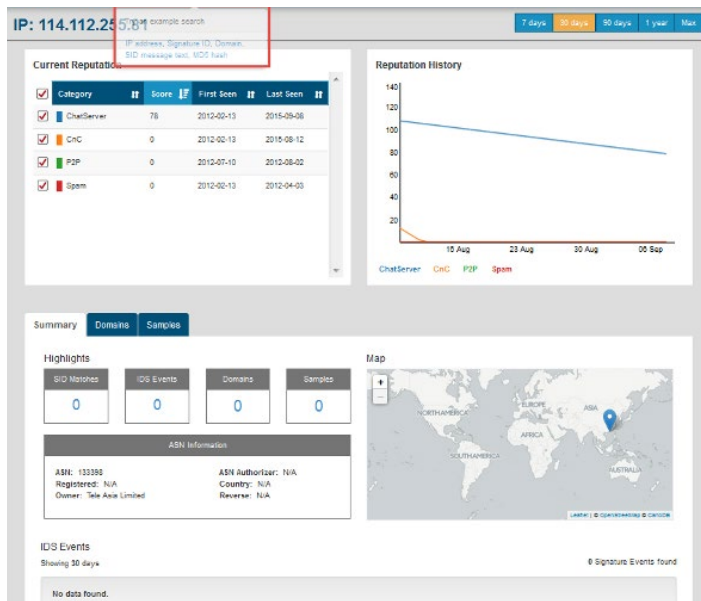

Figure 2: ET Search

Time Range Selector

Threats and actors change dramatically over time, and it is important to maintain the right context for researching how these impact your environment. The Time Range Selector gives you the power to view the threat landscape over different periods of time. The default timeframe is 30 days. The selector will not only impact what is displayed in the Reputation History Graph, but it also will impact what content is displayed for other areas. For instance, this will filter how far back IDS Events, Samples, Domains, and other content will be shown.

Viewing different time ranges:
ET Intelligence will score an event based upon the source, the confidence, and other factors such as the offending behavior. This gives an IP an initial reputation. If there is no other activity, then IP's reputation score will decay over a short period of time. If activity persists then there the reputation will be refreshed. This helps ensure that a machine that was compromised and then remediated will not be forever condemned, nor will that be the case for an IP or domain which may have been malicious at some point, but then cleaned up or repurposed. However it allows us to ensure that sources that are actively malicious are still properly represented.
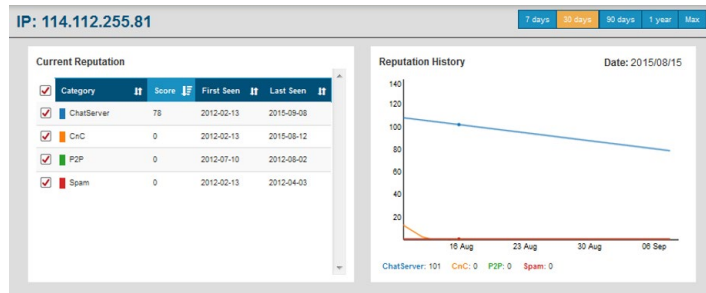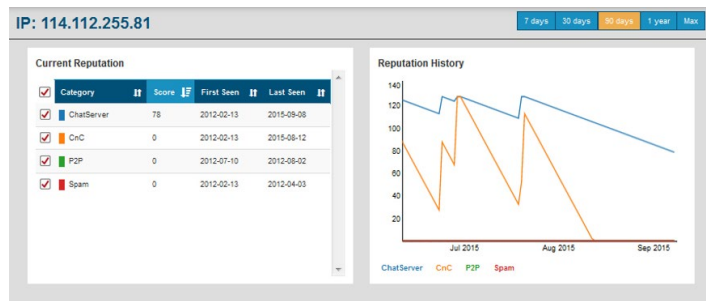

Figure 3: 30 Day Default View Example
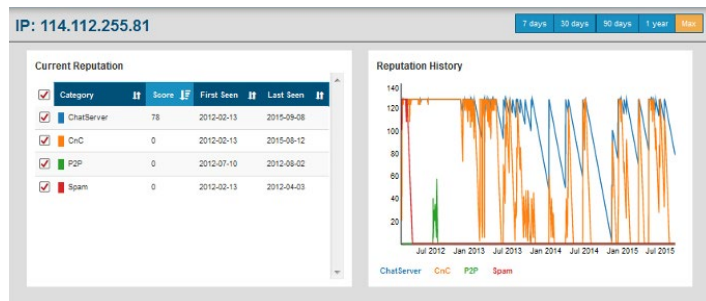

Figure 4: 90 Day Example

Figure 5: Max Reputation History Example

Note that you can also click on the checkboxes in the Current Reputation Table to select what categories show up in the graph. This can be useful when there are multiple categories or you are only concerned with one type.
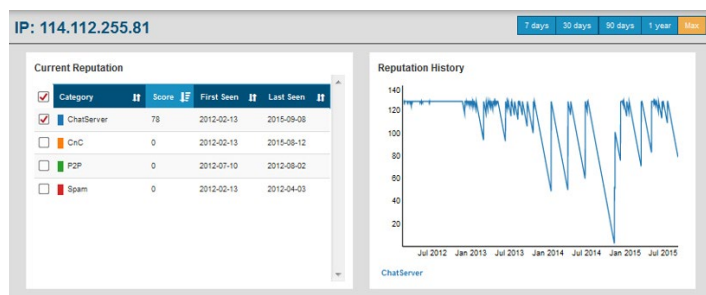

Figure 6: Max Reputation with Individual Category Selection

FEATURE BENEFITS

Anyone can produce a list of IP addresses. It's the story behind the list that is interesting—and most often missing. The goal of ET Intelligence Query is to stop the dead-end nature of most threat intelligence sources and illuminate all of the evidence behind why an IP address should be investigated in the first place. With the IP Search feature, we provide the needed context surrounding an IP going back historically as far as four years.

IP Reputation History can tell a detailed story of an IP addresses behavior and use over time. Often a combination of categories can identify with high fidelity: malicious actors, their tools, and their intentions.

IP IDS events provide a direct connection to IP Reputation history. The information within this section is where a category like CnC is expanded to include the malware family name, its protocol, and often its intention—all in the language of the ETPro and ETOpen rule set. The type of rules an IP address fires is one of the biggest factors in the assignment of reputation category.

Related samples and domains help close the loop in an investigation where information is missing. Maybe you have the sample, but need the call back IP addresses to stop or identify infection. Related data means that indicators of compromise (IOC) will only rarely be isolated.

Armed with this data, and the other information provided on the IP Address search page, the user will be able to see a detailed story behind each IP, relate it to many different IOCs, and get a better understanding of the risk presented by IP addresses in this ASN.

IP Address Search

ET Intelligence Query allows the user to search for any public IPv4 address. The search will provide the historical ET view of an IP address object, and at the very least the ASN information for any IP. IP's with any reputation will also show a great deal of information.

The information is represented in a tabbed layout to help provide at a glance understanding of an object so you can quickly and effectively determine if you are interested in this object or if it is not interesting and you can move on. As part of this we feature the following tabs:

• Summary: Contains high level information about the event counts for each of tracked attributes (Domains, Samples, SID Matches, and IDS Events) as well as:
  - ASN Data
  - IDS Events: Events that were triggered by this IP
  - GeoLocation Map: Shows where the IP is hosted.
• Domains: Contains information about any domains mapped to this IP address
• Samples: Contains a list of any samples which have been observed from this IP address.

If no information exists for the IP address searched, the user will see "No data found" in place of the respective data tab.
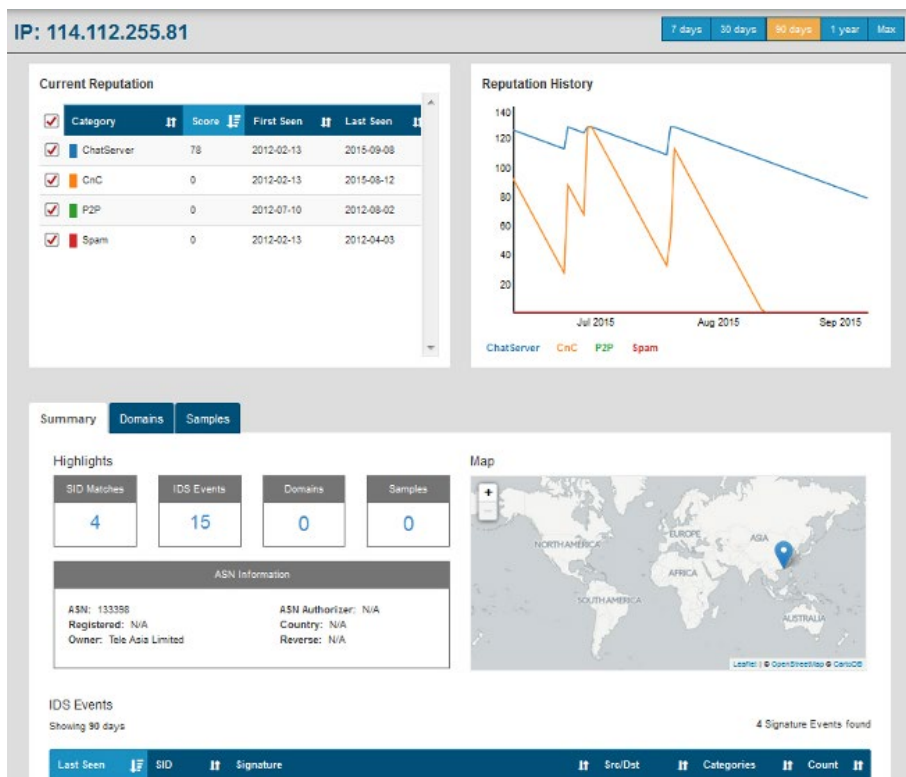

Figure 7: ET Intelligence Portal

Current Reputation Score:

An element is given a "confidence score" within each category. This score is not a quantitative assignment of risk, but rather reflects the degree of confidence that Emerging Threats has that the IP Address is exhibiting the behavior associated with that category. Categories include negative, neutral, and positive behaviors, and are designed for cross-correlation and context.

An IP address will often exist in multiple categories. Clicking on the Category name will toggle that category on the graph. Note that this is the current reputation score. Some categories will show as 0, regardless of the timerange selector as this is only a current not historical score like what is displayed on the graph.
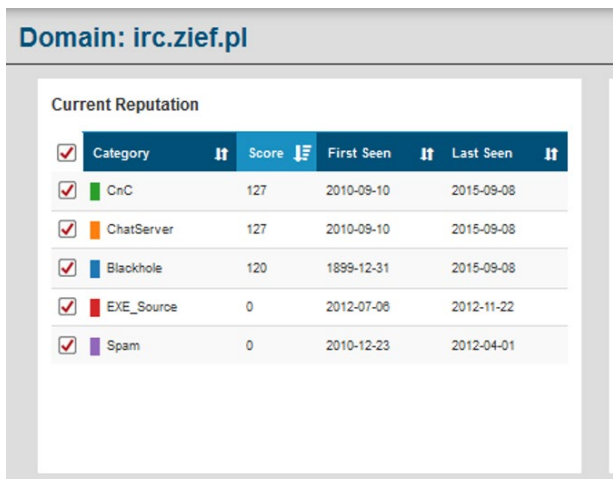

Figure 8: Current Reputation Score Table

Associated Domains

The "Domains" tab provides the user with domains that have been observed resolving to the searched IP address during that IP addresses history within the Emerging Threats system. It is important to understand that this data tab is not a WHOIS or passive DNS lookup. There may be more domains associated with an IP than display, but here Emerging Threats is presenting ONLY those domains that have been observed in the DNS process. This table also allows you to search sort based on first/last seen information, or to click on any domain to drill down.
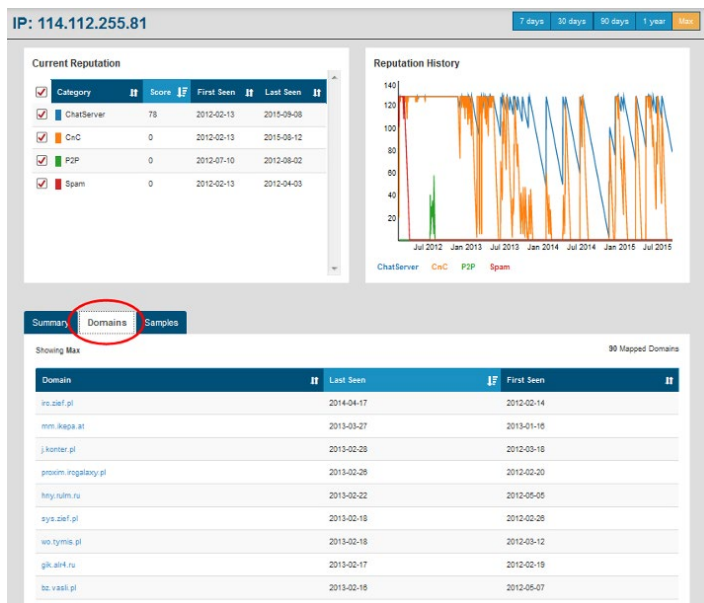

Figure 9: Associated domains

Related Samples

Related samples Emerging Threats has collected over the last several years. The related samples are samples which are tied to the objects being viewed. For instance, if a malicious MD5 was tracked to a given IP because a download was seen being served from that IP. The samples table includes the ability to do sorting on each column, and features information about when the sample was first seen, last seen, and what the current Virus Total Detection Ratio is for that sample. You can click on the Virus Total Detection Ratio to go to the Virus Total site for more information.
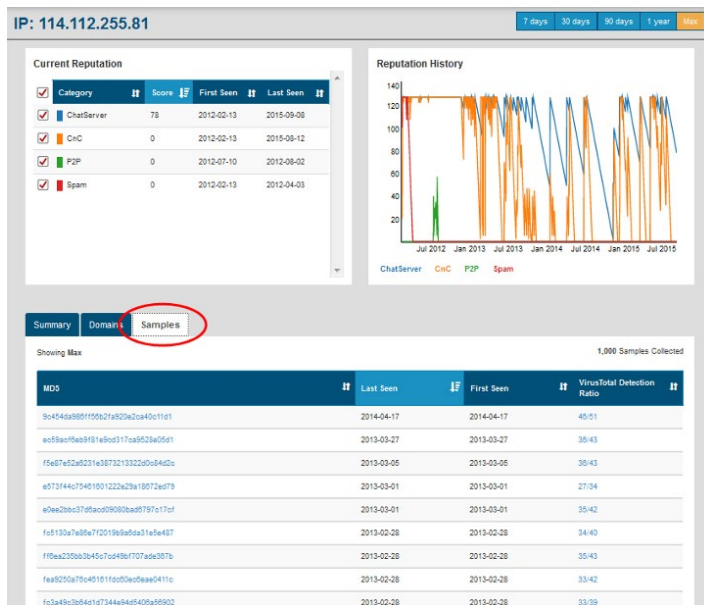

Figure 10: Related Samples

IDS Events

ETPro and ETOpen IDS Events which were triggered in the wild, and sent to the global ET SensorNet. The table features not only the signatures and a link to the signature for more information, but also information about the category for the signature, the hit count for the time period selected, and the direction the attack was detected.
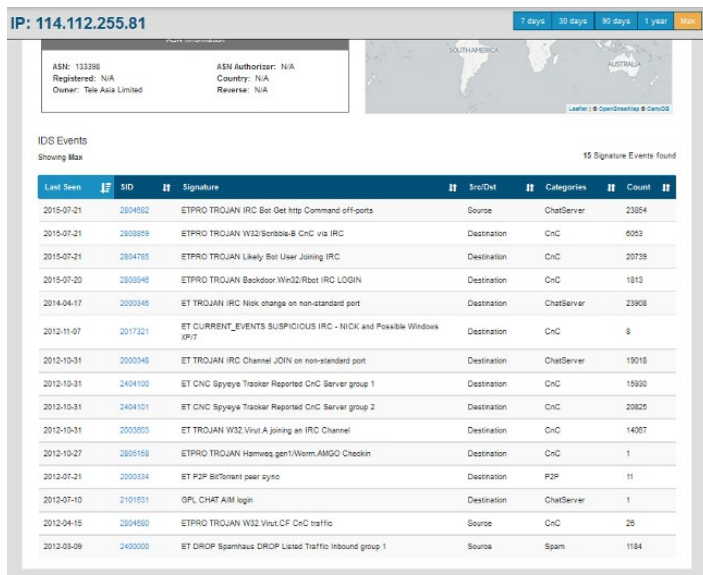

Figure 11: IDS Samples

Domain Search

Similar to the IP Address search, ET Intelligence Query allows the user to search for fully qualified domain names as well as domain plus or surrounded by the star * wildcard (i.e. *mydomain*). If the domain exists, WHOIS information will be returned. If the domain searched is one of the millions contained in the Emerging Threats system of worldwide collection and malware analysis it will be returned.

The information is represented in a tabbed layout to help provide at a glance understanding of an object so you can quickly and effectively determine if you are interested in this object or if it is not interesting and you can move on. As part of this we feature the following tabs:

- Summary: Contains high level information about the event counts for each of tracked attributes (Domains, Samples, SID Matches, and IDS Events) as well as:
  - Registrar/Registrant: Who registered the domain and with whom?
  - IDS Events: Events that were triggered by this IP
  - GeoLocation Map: Shows where the IP is hosted.

- IP: Contains information about any IPs mapped to this domain
- Samples: Contains a list of any samples which have been observed from this domain
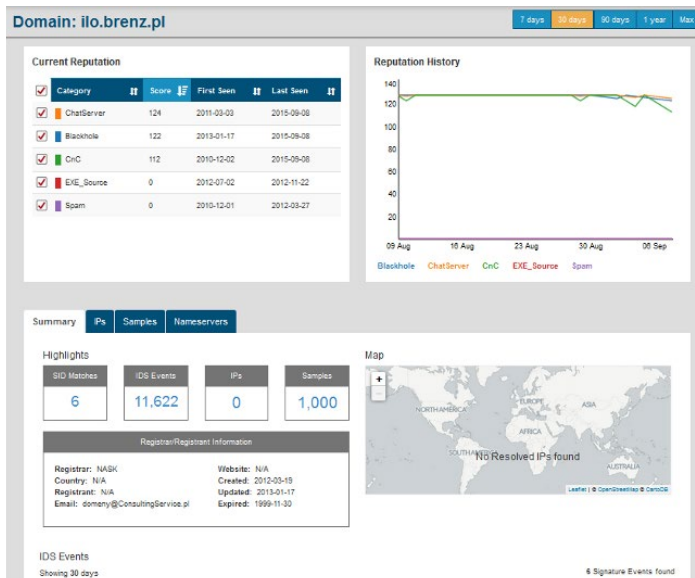- Nameserver: Who is the authoritative nameserver for this domain

Figure 12: Domain Search Results

Domain Reputation History

Domain Reputation History provides the user with the elements' categorical history within the Emerging Threats ET Intelligence Reputation system. The product of worldwide sensor placement, and massive malware sample collection and analysis, ET Intelligence Reputation assigns an element with one of 40 categories, and a score within that category. See Appendix A for a list and description of ET Intelligence Rep list categories.

An element is given a "confidence score" within each category. This score is not a quantitative assignment of risk, but rather reflects the degree of confidence that Emerging Threats has that the domain is exhibiting the behavior associated with that category. Categories include negative, neutral, and positive behaviors, and are designed for cross-correlation and context.

A domain will often exist in multiple categories. Clicking on the Category name will toggle that category on the graph at the left.

Associated IPs

The "IPs" tab provides the user with IP addresses that have been observed resolving to the searched domain during that domains history within the Emerging Threats system. It is important to understand that this data tab is not a WHOIS or passive DNS lookup. There may be more IPs associated with a domain than displayed, but here Emerging Threats is presenting ONLY those IPs that have been observed in the DNS process.

FEATURE BENEFITS

As with the IP address search, domain search provides the story behind the domain, and the evidence supporting its inclusion within an ET Intelligence Reputation list. Unlike the list, ET Intelligence Query will serve up domains that have been within the reputation system for up to four years, and not just those domains producing active scores that day. With access to this type of data, a user can investigate incidents that may have happened months in the past, as well as anticipate actions by actors well into the future.

The goal is to provide full context: who, what, where, when, why and how. Registrar, Registrant, and Nameservers help provide information about who. Unlike an IP address, a domain typically represents a single actor, as opposed to a shared environment. The registrant information can help a user cluster other domains by this actor and possibly relate them to known actions or intentions. An actor's calling card is often their Nameservers, and while the domains they register may be many, they often point them to the same Nameservers under their control.

The combination of Domain Reputation History and IP IDS events helps close the loop for the what, when, why and how. Categories are behaviors directly related to IDS events. Think of a category like a summary of a unique selection of alerts chosen by Emerging Threats. The categories provide a summary and level of activity score, while the IDS events are the details. Accurate ETPro rules help the user see actions, intentions and the types of tools and exploits in use. And by using timestamp tools, ETPro can determine when the methods were used.

Each tile of information within domain search presents the user with ways to relate other IOCs together. Samples can be related to domains and then the actor in the registrant detail. URLs can more uniquely identify malicious methods, while domain geolocation can present the user with an actors worldwide operational model.

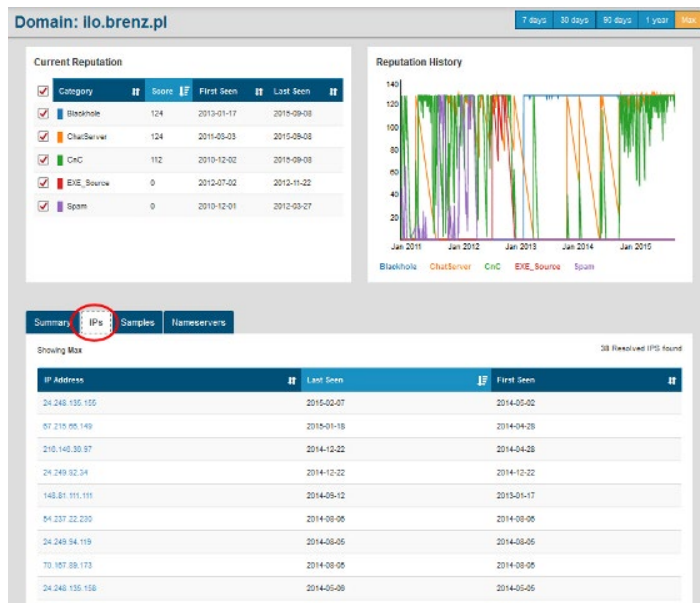With the full story, investigations can end quicker, IOCs can be shared and actions can be prioritized.

Figure 13: Associated IP Addresses

Nameservers

The servers that respond with the IP address of the domain in question. Note that this can change over time. In Figure 16, the nameserver has been changed to a sinkhole as the domain has been condemned.
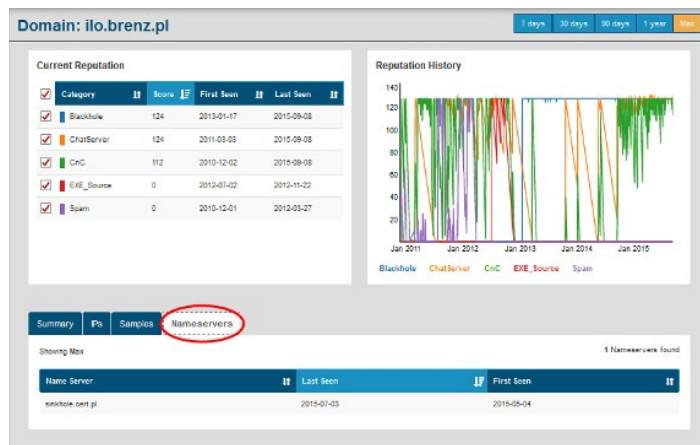

Figure 14: Associated Nameservers

Related Samples

Related samples Emerging Threats has collected years of threat samples which contain an instance of the searched domain within the network traffic captured by Emerging Threats when the sample was executed on a virtual host. Clicking on a hyperlinked sample will produce a sample search, and take the user to the Sample Analysis page.
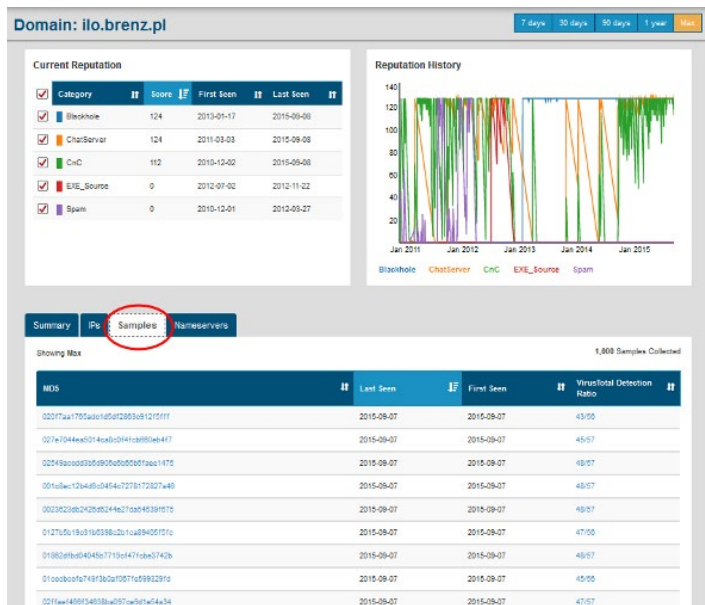

Figure 15: Related Samples

IP IDS Events

ETPro and ETOpen IDS Events fired by the IP address that the searched domain resolved to during the Sandnet execution process. Here the IP that fired the alert will be a destination IP address. The hyper link to the left is the Emerging Threats SID (signature identifier), and can be clicked to take the user to a SID search. The signature column presents the user with the MSG field of the actual rule.
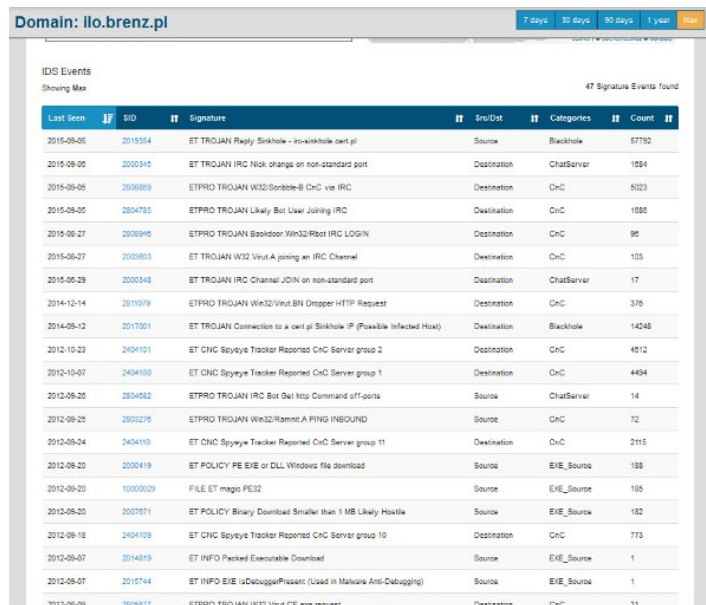

Figure 16: IDS Events

FEATURE BENEFITS

The network doesn't lie. Today, advanced malware can evade endpoint antivirus. The ET Intelligence Query Sample Search feature was designed to present the user with an unbiased and untainted view of malware in motion—from a perspective that is harder to tamper with.

The sample analysis page provides the user with the same type of information that our world-class research team uses to write the ETPro ruleset. The user is presented with four different perspectives on network traffic. Each perspective arms the user with a chance to catch anomalies that might not be detected by the prior tab.

Even in situations where no alerts are fired, the user is still given many options to detect, or relate to other IOCs in order to continue an investigation that had reached a dead-end.

Sample Search

ET Intelligence Query allows the user to search based upon the MD5 hash of a sample in the Emerging Threats sample database. Emerging Threats possesses hundreds of millions of samples that include DLL files, PDFs, EXE files, MS Office documents and much more.

A sample search will take the user to the Sample Analysis page. The sample analysis page includes metadata about the sample, and a tabbed index of the network traffic that sample produced when executed on a host including the TCP/IP, DNS, and HTTP connections. A link to Virus Total using the searched sample is also provided at the bottom of the sample metadata field.

Figure 17: Sample Analysis Page

There are occasions where ET receives PCAP files that detail the network traffic of certain threats. In those situations, the sample analysis page will still index that traffic using the four tabs described below, the only difference is that the MD5 sum is that of the PCAP file and not the sample. Type, SHA256, and file size will be marked "NA." An example of this condition is below:

Sample Analysis Tabs include:

• Alerts
• Connections
• DNS
• HTTP

FEATURE BENEFITS

SID search offers perhaps the most powerful and compelling feature of the tool. ETPro signatures are the primary method in which ET as an organization, expresses itself. So if you were to ask ET, "What is this particular Exploit Kit doing these days," the response would be a collection of signature identifiers (SIDs). We could tell you what the landing page looked like, what redirection method they used, how they exploited java and what actions after compromise looked like—all using ETPro SIDs.

With this in mind the user is able to take SIDs from their alert console and get a global perspective on something that happened locally. Using SID search, the user could see related IOCs, actions, tools, and help piece together the intrusion kill chain that surrounds a single event they maybe looking at in a console.

Here the user is able to see the entire body of an attack before it happens so that they can align their defenses accordingly, or piece together an intrusion that already took place using the context provided by ET Intelligence Query.

Tab descriptions

Alerts

The Alerts tab displays the ETPro and ETOpen IDS Alerts that were fired while observing network traffic to and from the host during sample execution. Samples have unrestricted access to the internet during execution. All columns on the alerts tab can be sorted from high to low or low to high. Hyperlinked IP addresses can be clicked to arrive at an IP address Search. The search function of this tab will search rule MSG body and other fields.

Connections

The connections tab presents a list of connections made by the host that the sample was executed on. All columns on the connections tab can be sorted from high to low or low to high. Hyperlinked IP addresses can be clicked to arrive at an IP address Search.

DNS

The DNS tab presents a list of DNS transactions from the host that executed the sample in question. All columns on the connections tab can be sorted from high to low or low to high. Hyperlinked IP addresses and domains can be clicked to arrive at an IP address Search.

HTTP

The HTTP tab presents a list of the extracted HTTP headers based upon HTTP transactions performed by the host that executed the sample. All columns on the connections tab can be sorted from high to low or low to high. Hyperlinked IP addresses and domains can be clicked to arrive at an IP address Search.

SID Search

ET Intelligence Query allows a user to search based upon the ETPro or ETOpen Signature ID number. This search will return the associated IP addresses that have been seen fired the alert in question around the world and in the Emerging Threats proprietary Sandnet. IP addresses can be sorted to produce a sequential list.

Figure 18: SID Search

SID search also produces the domains that have been observed associated with SID and IP address pairings within the Emerging Threats proprietary Sandnet. A list of associated samples is also presented that when clicked produces a Sample analysis of the MD5.

Search History

In the Threat Intelligence system, we now provide a Search History capability which allows you to easily sift back through any searches which you, or anyone in your organization have done in ET Intelligence. This is very helpful for working cooperatively with others as well as recalling past searches. Simply click on the Search History button at the top of the screen. You can also click on any of the search terms to be brought to the current page for that object.

Figure 19: Search History

Appendix A

Categorization legend

Each ET Intelligence Rep List entry is given one of the following categories, and is displayed in the list with its corresponding category number:

1, CnC, Malware Command and Control Server

2, Bot, Known Infected Bot

3, Spam, Known Spam Source

4, Drop, Drop site for logs or stolen credentials

5, SpywareCnC, Spyware Reporting Server

6, OnlineGaming, Questionable Gaming Site

7, DriveBySrc, Driveby Source

9, ChatServer, POLICY Chat Server

10, TorNode, POLICY Tor Node

13, Compromised, Known compromised or Host

15, P2P, P2P Node

16, Proxy, Proxy Host

17, IPCheck, IP Check Services

19, Utility, Known Good Public Utility

20, DDoSTarget, Target of a DDoS

21, Scanner, Host Performing Scanning

23, Brute_Forcer, SSH or other brute forcer

24, FakeAV, Fake AV and AS Products

25, DynDNS, Domain or IP Related to a Dynamic DNS Entry or Request

26, Undesirable, Undesirable but not illegal

27, AbusedTLD, Abused or free TLD Related

28, SelfSignedSSL, Self Signed SSL or other suspicious encryption

29, Blackhole, Blackhole or Sinkhole systems

30, RemoteAccessService, GoToMyPC and similar remote access services

31, P2PCnC, Distributed CnC Nodes

32, SharedHosting, Known Shared Hosting server

33, Parking, Domain or SEO Parked

34, VPN, VPN Server

35, EXE_Source, observed serving executables

37, Mobile_CnC, Known CnC for Mobile specific Family

38, Mobile_Spyware_CnC, Spyware CnC specific to mobile devices

39, Skype_SuperNode, Observed Skype Bootstrap or Supernode

40, Bitcoin_Related, Bitcoin Mining and related

41, DDoSAttacker, DDoS Source

Periodically we add and retire categories from the published lists. To date, we have kept data and reputation attribution mechanisms active and associated with 40 different categories. Some categories, however, may be retired from publishing because it is more effective to globally safelist trusted sites instead of having them as a category. For others, we have removed categories that might be confusing or not relevant. In each case we may continue to track and maintain the category, but not publish it—this allows us to tweak attribution mechanisms, as well as create categories for R&D purposes.

Background & legend for each category:

1, CnC, Malware Command and Control Server
Observed or DGA predicted domains and IPs that are command and control for known Trojans. These listings are specifically criminal, differentiated from spyware and user tracking domains, which are classified in SpywareCnC.

2, Bot, Known Infected Bot
A host observed checking in to a command and control server, or exhibiting clear indications of unwanted and criminal code on the host.

3, Spam, Known Spam Source
We don't track all spam sources, but those observed sending spam or being rejected as blocklisted are included.

4, Drop, Drop site for logs or stolen credentials
Differentiated from CnC servers, but sometimes overlapping. Anywhere we see stolen data or credentials being pushed. Does not include droppers being served or other exe movement.

5, SpywareCnC, Spyware Reporting Server
Servers and domains observed being used to serve or track user activity. Specifically not clearly criminal, but we avoid plain ad-serving sites as much as is possible. Generally these are going to be toolbars, rogue gaming, free screensavers and more.

6, OnlineGaming, Questionable Gaming Site
Gambling, flash games, and similar that installs a client and report or track user activity. Most of these do not cross the line of criminal, but are differentiated from plain spyware activity.

7, DriveBySrc, Driveby Source
Kit redirectors, exploit serving, or injected or compromised sites that either have attempted to or will lead to a compromised browser. DriveBySrc is a category representing sites that have been utilized by various exploit kits such as Neosploit or Blackhole, where via some sort of HTML injection, a users browser is redirected to these sites that deliver an exploit by java or some other method.

9, ChatServer, POLICY Chat Server
Observed chat activity, including but not limited to IRC, Jabber, Google Talk, MSN, AIM, ICQ, Baidu, GaduGadu and more. This is not an indication of hostab activity, only known chat activity. Can be cross-correlated with CnC to help mitigate legitimate IRC networks in use as CnC.

10, TorNode, POLICY Tor Node
Identification of Tor exit nodes and participants seen in the network.

13, Compromised, Known compromised or Hostab
A bit of a catchall category for hosts that are observed hostab including compromised web servers, brute forcers, or otherwise not easily classifiable activity.

15, P2P, P2P Node
Observed clients and sources of generally legitimate file sharing, including traditional bittorrents, limewire or kazaa, qvod and others.

16, Proxy, Proxy Host
Observed proxy endpoint for http, stun, socks and more.

17, IPCheck, IP Check Services
IP and geo check services. Generally public services which are very often abused by malware or dyndns activity.

19, Utility, Known Good Public Utility
Known good nets and services such as Google search frontends, Bing and more.

20, DDoSTarget, Target of a DDoS
Observed DDoS targets by traffic or observed commands to launch attacks to these nets.

21, Scanner, Host Performing Scanning
Web vulnerability scanning; open relay scanning, network and service recon, and often Nessus or other scanner activity.

23, Brute_Forcer, SSH or other brute forcer
All observed authentication brute forcing, including SSH, imap, VNC and more.

24, FakeAV, Fake AV and AS Products
Fake antispyware and av product sites being sold or distributed. Often overlaps with CnC.

25, DynDNS, Domain or IP Related to a Dynamic DNS Entry or Request
Host or domain observed using DynDNS.

26, Undesirable, Undesirable but not illegal
Some hack tool forums, metasploit updates and more. Not illegal, but of interest on an otherwise controlled network.

27, Abused TLD, Abused or free TLD Related
Activity or DNS related to rogue TLD and GTLDs such as .tk, co.cc, and others. Not always hostab, but of interest. Reserved for rogue registrars…registrars that either can't, or choose not to police their domains, and TLDs that are free or with less accountability. The TLD .su is a perfect example. ICANN can't claim a domain back from a country (Soviet Union) that no longer exists. Malicious activity in this category isn't certain, but typically suspicious.

28, SelfSignedSSL, Self Signed SSL or other suspicious encryption
Self-signed or other invalid SSL certificates in use.

29, Blackhole, Blackhole or Sinkhole systems
Known sinkhole in use by a trusted organization. Will often overlap with CnC.

30, Remote Access Service, GoToMyPC and similar remote access services
Observed but often legitimate remote access services like Kaseya, Gotomypc, Citrix, and others.

31, P2PCnC, Distributed CnC Nodes
Zeus and other families that use P2P as a CnC mechanism. Separated category to handle the volume and transient nature of these hosts.

33, Parking, Domain or SEO Parked
Known parked domain or parking server.

34, VPN, VPN Server
VPN protocols observed using this address as a concentrator. Potential anonymizing service.

35, EXE_Source, Observed serving of an Executable. Not necessarily hostab, but will often coincide with CnC.

40, Bitcoin_Related is a category based upon observed activity related to P2P Bitcoin mining. The focus here is not a user making transactions with Bitcoins, but actual Bitcoin clients running in the Bitcoin P2P network. This can help identify the rogue use of computing resources in Bitcoin mining operations.

41, DDoS Attacker, Source of DDoS traffic.

LEARN MORE

For more information, visit **proofpoint.com**.