Automated Context and Incident Response

Incident response requires situational awareness of the target, his or her environment, and the attacker. However, security alerts from most existing security systems provide high-level, normalized, generic, or unverified information that is not actionable. In addition, incident responders may not want to block every threat reported since many modern attackers use evasive techniques that include attempted connections to destinations like Microsoft update sites, Adobe update sites, Google searches, and Google DNS to mislead automatic systems. These and other evasive tactics complicate the incident response process and force security analysts to do more work.

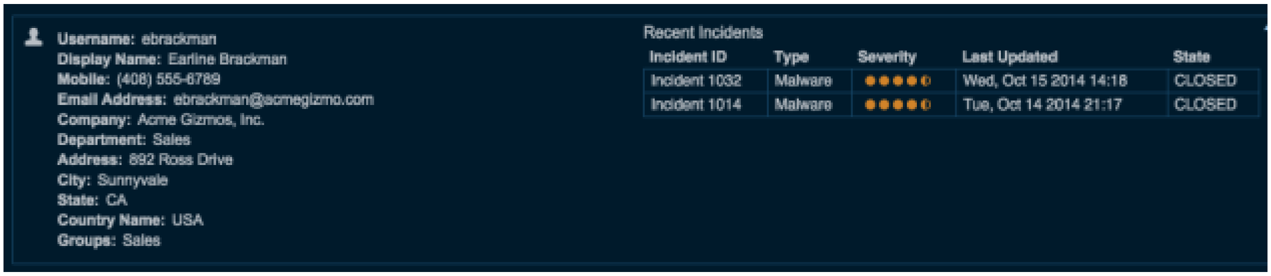
Incident responders need context. Context provides the:

- Who
- What
- Where

Adding deeper threat context enables the assignment of priority and accelerates the decision making for efficient incident response.

Who:

Who is involved in the incident? Is the person in the finance department? Is the person an executive? Is this person working in the mailroom?



Username: ebrackman
Display Name: Earline Brackman
Mobile: (408) 555-6789
Email Address: ebrackman@acmegizmo.com
Company: Acme Gizmos, Inc.
Department: Sales
Address: 892 Ross Drive
City: Sunnyvale
State: CA
Country Name: USA
Groups: Sales

Recent Incidents

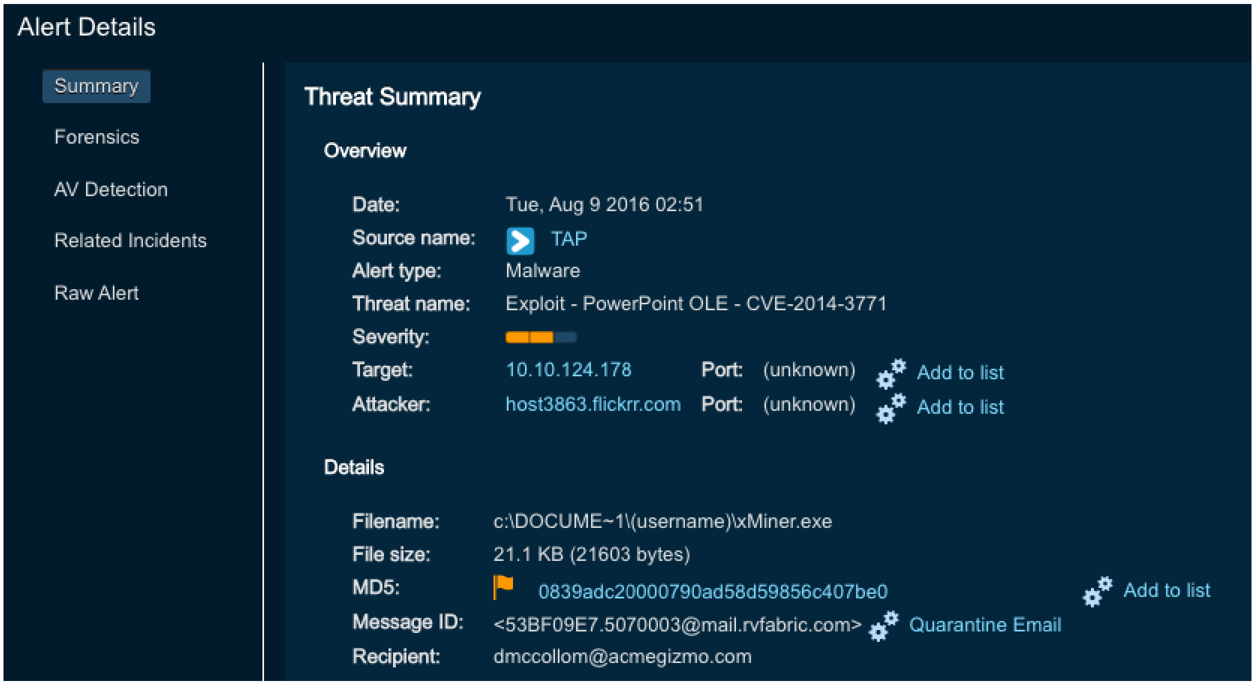
Incident ID	Type	Severity	Last Updated	State
Incident 1032	Malware	●●●●◐	Wed, Oct 15 2014 14:18	CLOSED
Incident 1014	Malware	●●●●◐	Tue, Oct 14 2014 21:17	CLOSED

Context tells you if key personnel such as the CFO or source code manager are involved in an incident, because if so, the threat should be taken more seriously. (In contrast, if the incident involves a mailroom employee who does not have any special login credential privileges to sensitive database information, then the threat may be less serious.) If you don't have context, you might prioritize each threat or security alert equally, when you should be focusing on the users or systems with the biggest impact on revenue, operations, or reputation.

Additional context of “who” in this case can include actionable information such as the phone number, physical location, reporting structure, and even the past incidents related to the user and their system. Using this information, analysts can act more quickly to alert, train, schedule a forensics review, quarantine, or otherwise rapidly take action on the system or user.

What:

What type of attack is this? Is it a Trojan, click fraud, or spam attack? Is it a credential phish? What type of malware was used? Is it a key logger, source code stealer, bank account screen sharer, or other?



Threat Summary

Overview

Date: Tue, Aug 9 2016 02:51
Source name: TAP
Alert type: Malware
Threat name: Exploit - PowerPoint OLE - CVE-2014-3771
Severity:
Target: 10.10.124.178 Port: (unknown)
Attacker: host3863.flickrr.com Port: (unknown)

Details

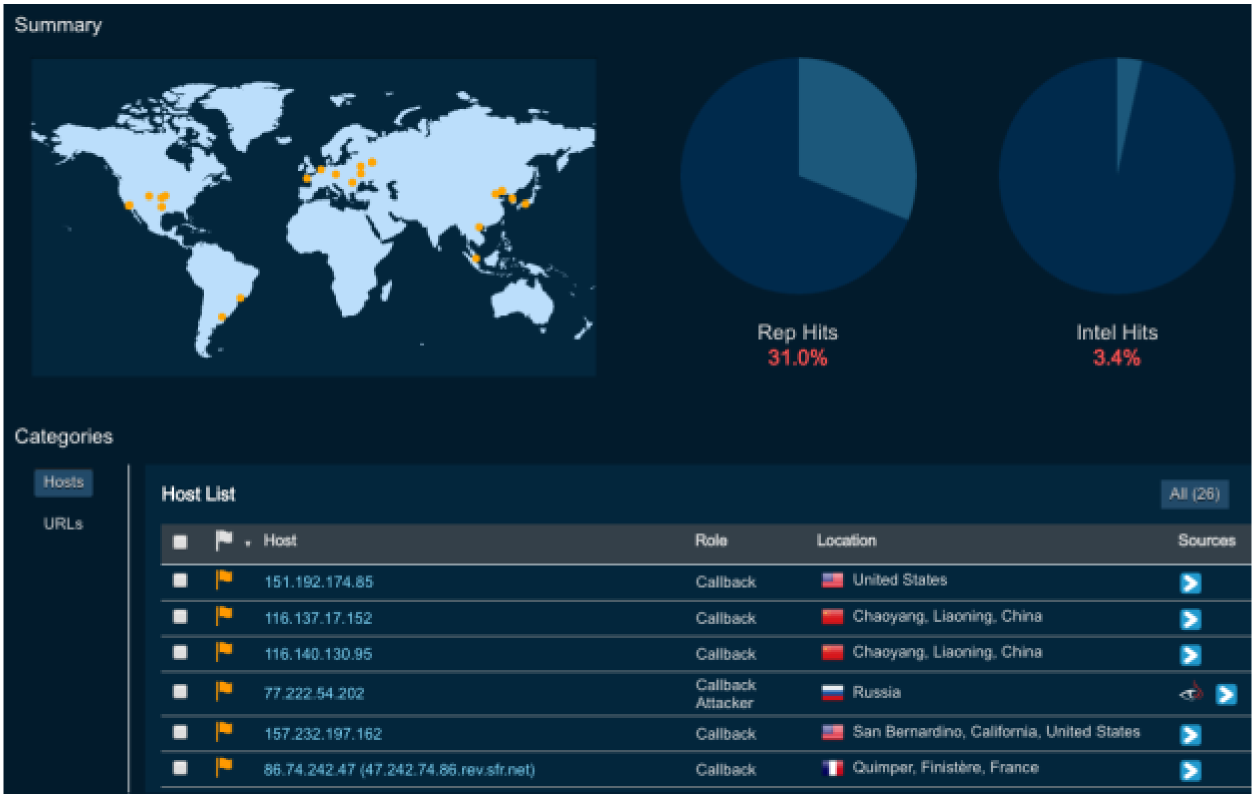
Filename: c:\DOCUME~1\(username)\xMiner.exe
File size: 21.1 KB (21603 bytes)
MD5: 0839adc20000790ad58d59856c407be0
Message ID: <53BF09E7.5070003@mail.rvfabric.com>
Recipient: dmccollom@acmegizmo.com

Context of the “what” tells you what tools or methods an attacker is using to compromise your organization. Certain malware and exploit kits target known vulnerabilities and include specific actions, such as trying to gain administrative privileges, inserting content on bank pages to steal credentials, clicking on ads, logging keystrokes, or taking other criminal actions.

Understanding the “what” context also helps prepare the security team for potential fraudulent action, the data loss, downtime, or system disconnects.

Where:

What sites, domains, or geo-locations are involved in the attack or incident? Do those sites have a reputation?



■	⚑	Host	Role	Location	Sources
■	⚑	151.192.174.85	Callback	United States	▶
■	⚑	116.137.17.152	Callback	Chaoyang, Liaoning, China	▶
■	⚑	116.140.130.95	Callback	Chaoyang, Liaoning, China	▶
■	⚑	77.222.54.202	Callback Attacker	Russia	▶
■	⚑	157.232.197.162	Callback	San Bernardino, California, United States	▶
■	⚑	86.74.242.47 (47.242.74.86.rev.sfr.net)	Callback	Quimper, Finistère, France	▶

Context of the “where” helps identify connections to sites, domains, and locations that you or people from your organization may make due to a possible malware infection or attack. In this context, a new or short-lived domain could be suspicious, just as accessing a site in North Korea or in Tunisia might seem suspicious. In addition, third-party reputation and threat intelligence feeds can be used to identify already known bad actors’ sites, domains, and URLs and use those to identify bad actors.

Caution should be applied here: security analysts need to be especially careful due to the recent trends in strategic web compromises and watering holes. In these cases, known good sites are temporarily infected and the security analysts cannot or should not block the sites permanently. For example, some malware will attempt to connect to 8.8.8.8, which is a Google DNS. If an incident response analyst does not know that a particular IP has an important function, they might block it and negatively impact many corporate users or other devices that depend on that Google DNS.

Automated Context Collection and Threat Scores

Proofpoint Threat Response goes several steps beyond collection of basic context. First, Threat Response collects the context of the who, what, and where in a consistent, reliable, and automated process. Next, Threat Response also collects indicators of compromise from targeted systems and confirms if a threat has compromised an endpoint.

The collected context and indicators of compromise are then analyzed in a regular and consistent manner to extract singular incidents out of multiple events. For example, if an incident is comprised of 15 related events, the net benefit is that instead of 15 independent analyses for those 15 events, only one analysis is done on a single incident with all the supporting the event information provided at a glance.

In addition, all the events that comprise an incident are analyzed, weighted, and then combined to create a threat score. This threat score – also calculated automatically – can enable organizations to assign analysts to the highest scoring and riskiest incidents first. Note: All of these steps are completed by Threat Response even before a security analyst begins to work on an incident analysis.

Applied Automated Context

Context is critical for incident response, however, automated context and analysis provides an even faster, more reliable, and more consistent method to deliver situational awareness. This sets the stage for correlating incidents from a number of related events, and enables a reliable and consistent scoring method to prioritize incident response assignments and workflow for analysts. The result is accelerated response decision making which lowers risk and exposure for an organization.