What’ s new in ThreatScape?

By Joshua Rosenthol

October 22, 2015

iSIGHT Partners

If you missed our recent webinar with Rick Holland from Forrester Research, check out the recording here. Rick provided a sneak peek into Forrester’ s upcoming Threat Intel Market report that will be published shortly. He described five key tenets that distinguish threat intelligence providers:

- Planning and direction
- Collection
- Processing
- Analysis and production
- Dissemination

We whole-heartedly agree with Rick’ s analysis. His tenets are not only a good way to differentiate intelligence providers but they also offer good segue to introduce you to our latest ThreatScape innovations. The changes we made span the tenets.

Our latest ThreatScape enhancements are particularly important for Security

Operations Center (SOC) and Incident Response teams. We enabled much quicker access to new IOCs, provided additional tags and improved navigation across iSIGHT’ s rich intelligence. With these enhancements SOC and IR teams can quickly and more completely understand the threats they are facing, speed investigations and more fully respond to sophisticated attacks.

We want to thank our customer for the continued input. The following changes are already available to customers.

Accelerated IOC Delivery

In keeping with our ongoing focus of providing finished intelligence to customers with ever increasing speed and quantity, but with the same level of accuracy and context, we improved our end-to-end process and made important changes to our internal ThreatScape Intelligence Platform (TIP). TIP is our intelligence collection and analysis system. TIP integrates our human intelligence with open source and our automated technical collections–including botnet, DDoS, malicious infrastructure and malware tracking systems.

The internal process and technology enhancements we made reduced the time from detection to delivery of key IOCs through ThreatScape API **from days or hours to seconds**. These dramatic improvements have been made to an important subset of ThreatScape Cyber Crime IOCs and we will address additional ThreatScape products moving forward. While we significantly sped up indicator delivery, we maintained the accuracy and fidelity customers expect from iSIGHT. We absolutely understand the need for speed, but also know that if we fail to provide well-validated indicators or indicators with out context, SOC teams end up with the worst possible outcome–more alerts and alarms and no good way to prioritize them.

Enhanced Intelligence Relevancy

This feature enables customers to run automated queries and determine if they are being specifically targeted. We introduced a new “target” data tag that is defined as an entity targeted by malware or actor. This tag could denote a URL (web objects), IP (DDoS), Domain (DDoS, web injects), specific components on a website (application that triggers inject) and more.

Below is an example of an API query in Python using the new target tag. The query pulls the last fourteen days of targeting information from our finished intelligence holdings for the Dridex malware–used extensively in cyber crime campaigns.

```
public_key = ‘YOUR_PUBLIC_KEY’
private_key = ‘YOUR_PRIVATE_KEY’

time_stamp = email.Utils.formatdate(localtime=True)

search_time = datetime.datetime.now() - datetime.timedelta(days = 14)

search_time_in_epoch = int(time.mktime(search_time.timetuple()))

search_query = '/view/targets?since=' + str(search_time_in_epoch) + '&threatType=malwareFamily&value=dridex'

accept_version = '2.1'
accept_header = 'application/json'

hash_data = search_query + accept_version + accept_header + time_stamp
```

```
hashed = hmac.new(private_key, hash_data, hashlib.sha256)

headers = {
'Accept' : accept_header,
'Accept-Version' : accept_version,
'X-Auth' : public_key,
'X-Auth-Hash' : hashed.hexdigest(),
'Date' : time_stamp,
}
```

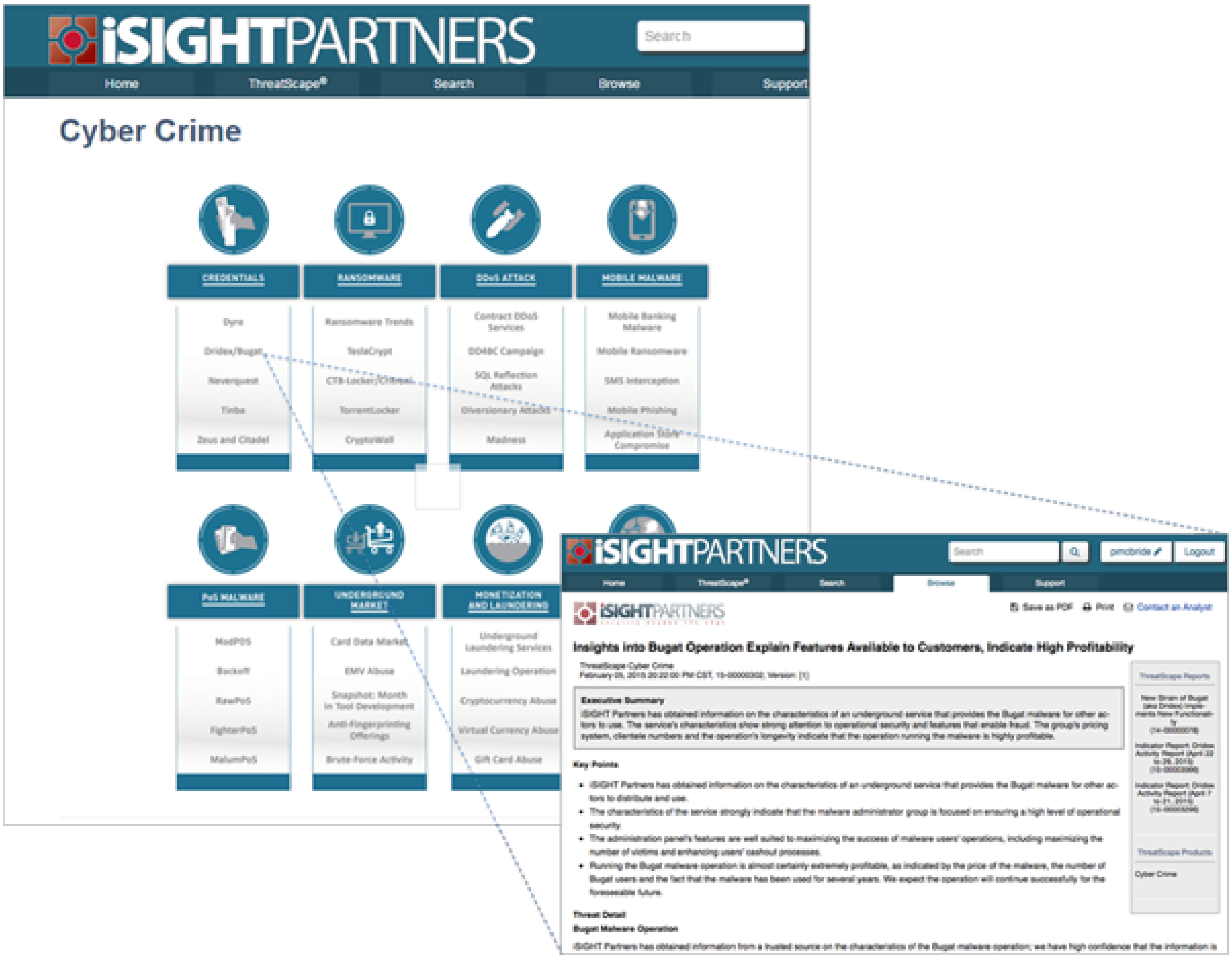
The query returns a list of target URLs, files or process that can be matched against your infrastructure to discern whether your organization is in the cross hairs. You can [download the full script here at iSIGHT Partners GitHub](#).

Please note: this new indicator is available via API 2.1 or later

Improved Accessibility to Threat Intelligence

We more tightly coupled ThreatScape intelligence and enhanced MySight portal navigation.

New graphical navigation panels that are linked to foundational intelligence called “profile” reports have been introduced in MySight. Each ThreatScape now has a graphical panel that links to profile reports on: actor profiles, malware families, underground forums, exploit kits, regional hacktivist groups or country profiles. See the example below from the Cyber Crime ThreatScape.



Insights into Bugat Operation Explain Features Available to Customers, Indicate High Profitability

ThreatScape Cyber Crime
February 05, 2015 20:22:00 PM CST, 15-00000302, Version: [1]

Executive Summary
iSIGHT Partners has obtained information on the characteristics of an underground service that provides the Bugat malware for other actors to use. The service's characteristics show strong attention to operational security and features that enable fraud. The group's pricing system, clientele numbers and the operation's longevity indicate that the operation running the malware is highly profitable.

Key Points

- iSIGHT Partners has obtained information on the characteristics of an underground service that provides the Bugat malware for other actors to distribute and use.
- The characteristics of the service strongly indicate that the malware administrator group is focused on ensuring a high level of operational security.
- The administration panel's features are well suited to maximizing the success of malware users' operations, including maximizing the number of victims and enhancing users' cashout processes.
- Running the Bugat malware operation is almost certainly extremely profitable, as indicated by the price of the malware, the number of Bugat users and the fact that the malware has been used for several years. We expect the operation will continue successfully for the foreseeable future.

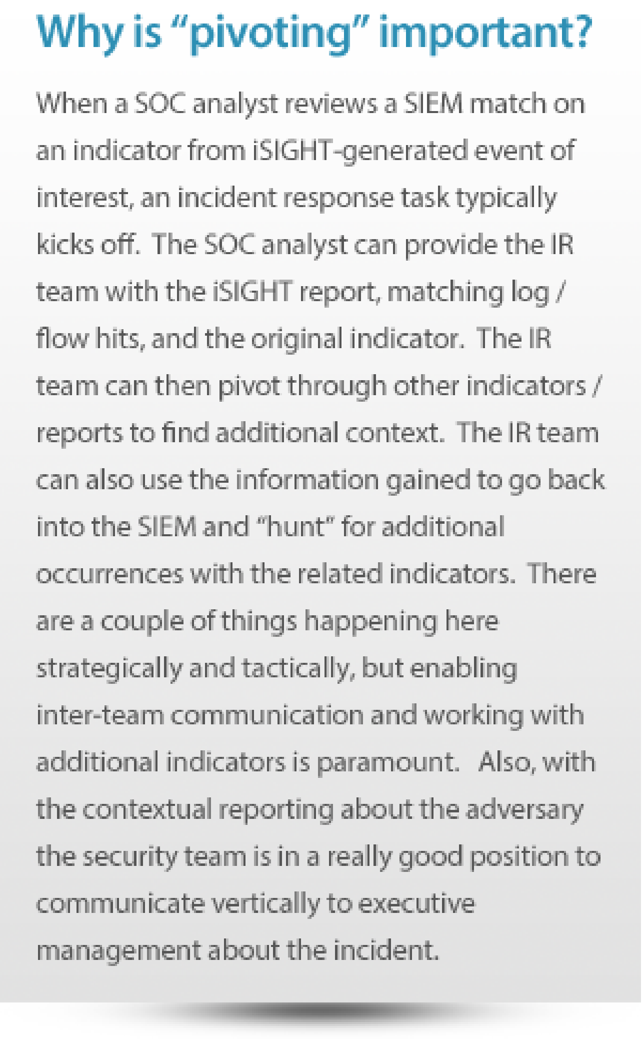
Threat Detail
Bugat Malware Operation
iSIGHT Partners has obtained information from a trusted source on the characteristics of the Bugat malware operation; we have high confidence that the information is

New Strain of Bugat (aka Dridex) Implements New Functionality (14-00000078)

Indicator Report: Dridex Activity Report (April 22 to 28, 2015) (15-00000[illegible])

Indicator Report: Dridex Activity Report (April 7 to 21, 2015) (15-00000[illegible])

We also introduced “related reports” in MySight. With related reports, you can easily navigate from a profile to a related report about that adversary, for example, or from an indicator back up to a profile report. These changes enable easier access to related threat intelligence that SOC and IR teams can leverage as they cull through events and investigate important threats.



Why is “pivoting” important?

When a SOC analyst reviews a SIEM match on an indicator from iSIGHT-generated event of interest, an incident response task typically kicks off. The SOC analyst can provide the IR team with the iSIGHT report, matching log / flow hits, and the original indicator. The IR team can then pivot through other indicators / reports to find additional context. The IR team can also use the information gained to go back into the SIEM and “hunt” for additional occurrences with the related indicators. There are a couple of things happening here strategically and tactically, but enabling inter-team communication and working with additional indicators is paramount. Also, with the contextual reporting about the adversary the security team is in a really good position to communicate vertically to executive management about the incident.

Pivoting is not only a MySight feature. As we noted in this blog, we introduced substantial pivoting capability built into ThreatScape API 2.0 in February.

For example, with some python scripting and the ThreatScape API you can now take an indicator such as an SHA256 hash and get additional hunting indicators and intel from reporting at the adversary level to assist in the response. This can also potentially provide clarity to previous incidents on your network if you pivot through your old incident information.

Have you migrated to API 2 yet?

In order to take advantage of the latest features and improvements, API 2.0 is required (or API 2.1 where indicated). If you have not upgraded to the latest API, we encourage you to do so. Read our blog on how to upgrade from API 1 to API 2.

If you have any questions about what’ s new and how to leverage it effectively, please don’ t hesitate to reach out to your Client Engagement Manager.

1 Share 1 Tweet 1 Share 0 Email 2 G+1

Want to learn more?

[Request a Consultation >]

[Interested in a FREE Trial? >]

[Download a Datasheet >]

Definitive Guide to Cyber Threat Intelligence
Cyber Threat Intelligence
We wrote the book.
Get your FREE Guide

Recent Posts

- What’ s new in ThreatScape?
- What do you mean you’ re not on API 2 yet?
- ThreatScape Media Highlights Update – Week Of October 21st

Michael Viscuso

CEO, Carbon Black

> iSIGHT’ s threat intelligence allows our users to prepare for, detect and respond to emerging threats all within one platform and without any additional effort.

Comprehensive cyber intelligence connecting security technology and operations to the business.
+1-214-731-4585 info@isightpartners.com

Privacy Policy