TXHunter – Automated Endpoint Forensic Threat Investigation Solution

THREAT HUNTING

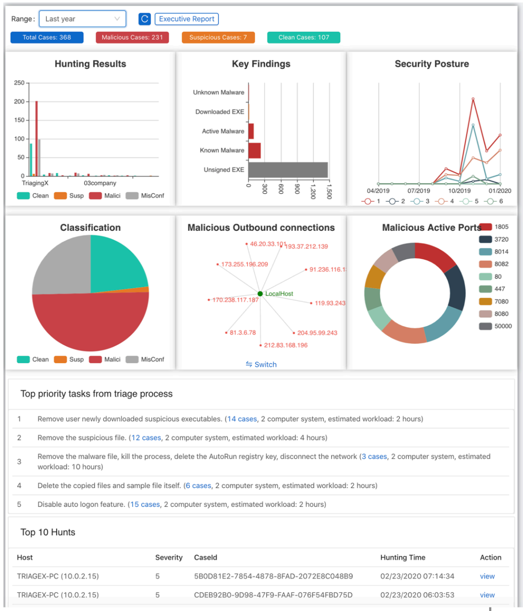
TXHunter automates endpoint threat forensic investigation process, not only detects deeply hidden advanced threat, but also detects potential risks, measures security postures and compliances status. No question to ask, no hypotheses required, not relying on documented IOCs. It is also integrated with EDR, SIEM and FW/IPS.

Deployment

TXHunter supports Windows and Linux platform, supports agent-less operation. TXHunter server can be deployed on-premises, or in public/private clouds.

SECURITY OPERATIONS

TXHunter enables security teams to verify in minutes, whether high value desktop or server have been compromised or exist potential risks. It supports online, offline and managed hunting modes. It supports proactive hunting and post infection hunting.



Top priority tasks from triage process

1 Remove user newly downloaded suspicious executables. (14 cases, 2 computer system, estimated workload: 2 hours)

2 Remove the suspicious file. (12 cases, 2 computer system, estimated workload: 4 hours)

3 Remove the malware file, kill the process, delete the AutoRun registry key, disconnect the network (3 cases, 2 computer system, estimated workload: 10 hours)

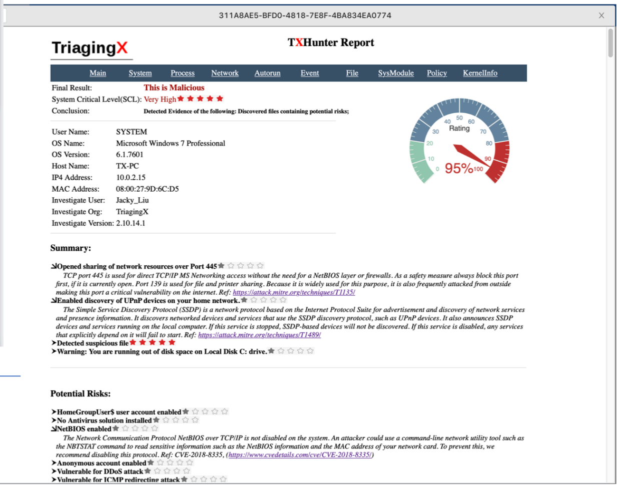
4 Delete the copied files and sample file itself. (6 cases, 2 computer system, estimated workload: 2 hours)

5 Disable auto logon feature. (15 cases, 2 computer system, estimated workload: 2 hours)

Top 10 Hunts

Host	Severity	CaseId	Hunting Time	Action
TRIAGEX-PC (10.0.2.15)	5	5B0D81E2-7854-4878-8FAD-2072E8C048B9	02/23/2020 07:14:34	view
TRIAGEX-PC (10.0.2.15)	5	CDEB92B0-9D98-47F9-FAAF-076F54FBD75D	02/23/2020 06:03:53	view

Completed Executive View



TXHunter Report

Final Result: This is Malicious
System Critical Level(SCL): Very High ★★★★★
Conclusion: Detected Evidence of the following: Discovered files containing potential risks;

User Name: SYSTEM
OS Name: Microsoft Windows 7 Professional
OS Version: 6.1.7601
Host Name: TX-PC
IP4 Address: 10.0.2.15
MAC Address: 08:00:27:9D:6C:D5
Investigate User: Jacky_Liu
Investigate Org: TriagingX
Investigate Version: 2.10.14.1

Summary:

Opened sharing of network resources over Port 445 ★☆☆☆☆

TCP port 445 is used for direct TCP/IP MS Networking access without the need for a NetBIOS layer or firewalls. As a safety measure always block this port first, if it is currently open. Port 139 is used for file and printer sharing. Because it is widely used for this purpose, it is also frequently attacked from outside making this port a critical vulnerability on the internet. Ref: https://attack.mitre.org/techniques/T1135/

Enabled discovery of UPnP devices on your home network. ★☆☆☆☆

The Simple Service Discovery Protocol (SSDP) is a network protocol based on the Internet Protocol Suite for advertisement and discovery of network services and presence information. It discovers networked devices and services that use the SSDP discovery protocol, such as UPnP devices. It also announces SSDP devices and services running on the local computer. If this service is stopped, SSDP-based devices will not be discovered. If this service is disabled, any services that explicitly depend on it will fail to start. Ref: https://attack.mitre.org/techniques/T1489/

Detected suspicious file ★★★★★

Warning: You are running out of disk space on Local Disk C: drive. ★☆☆☆☆

Potential Risks:

HomeGroupUser$ user account enabled ★☆☆☆☆

No Antivirus solution installed ★☆☆☆☆

NetBIOS enabled ★☆☆☆☆

The Network Communication Protocol NetBIOS over TCP/IP is not disabled on the system. An attacker could use a command-line network utility tool such as the NBTSTAT command to read sensitive information such as the NetBIOS information and the MAC address of your network card. To prevent this, we recommend disabling this protocol. Ref: CVE-2018-8335, (https://www.cvedetails.com/cve/CVE-2018-8335/)

Anonymous account enabled ★☆☆☆☆

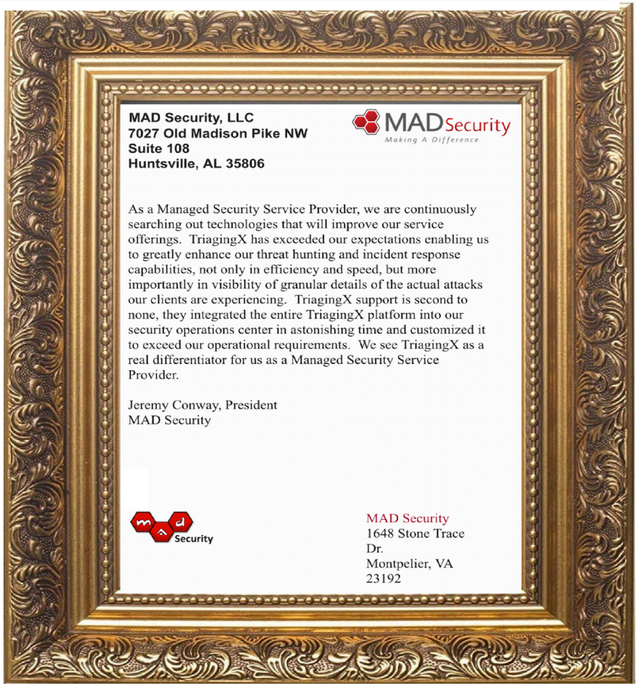
Vulnerable for DDoS attack ★☆☆☆☆

Vulnerable for ICMP redirecting attack ★☆☆☆☆

ATT&CK™
Adversarial Tactics, Techniques & Common Knowledge
MITRE
Persistence
Privilege
Escalation
Defense
Evasion
Credential

Feature Highlights

1. Conducts endpoint forensic threat investigation automatically and proactively
2. Integrates with EDR, SIEM, and FW/IPS
3. Follows Mitre security framework and fits well into the enterprise security operation flow
4. Detects hidden processes, APT and rootkits
5. Detects zombies and unknown malware with embedded sandbox behavior analysis
6. Detects cryptocurrency mining malware
7. Detects reverse shell and advanced attacks
8. Detects misconfigurations and potential risks
9. Detects ransomware and protects user data files
10. Measures endpoint security posture and compliance status at real time



MAD Security, LLC
7027 Old Madison Pike NW
Suite 108
Huntsville, AL 35806

MADSecurity
Making A Difference

As a Managed Security Service Provider, we are continuously searching out technologies that will improve our service offerings. TriagingX has exceeded our expectations enabling us to greatly enhance our threat hunting and incident response capabilities, not only in efficiency and speed, but more importantly in visibility of granular details of the actual attacks our clients are experiencing. TriagingX support is second to none, they integrated the entire TriagingX platform into our security operations center in astonishing time and customized it to exceed our operational requirements. We see TriagingX as a real differentiator for us as a Managed Security Service Provider.

Jeremy Conway, President
MAD Security

Security

MAD Security
1648 Stone Trace
Dr.
Montpelier, VA
23192

TriagingX Inc.

TRIAGINGX

TriagingX has extended the behavior analysis capability from sandbox for a single file object to the entire endpoint system, including desktop and server computers, physical or in the cloud. TXHunter automates forensic investigation for all alerts from firewall/IPS, SIEM and EDR. It detects deeply hidden advanced threats and potential risks through its behavioral forensics. It's fast, efficient, effective, consistent and always works.

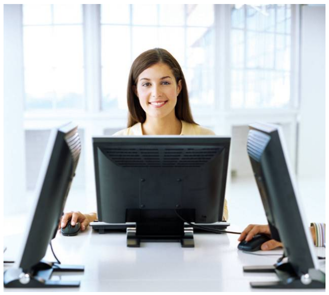
For more information on any of our products or services please visit us on the web at:

www.triagingx.com

Would you like to see a demo? Please write to

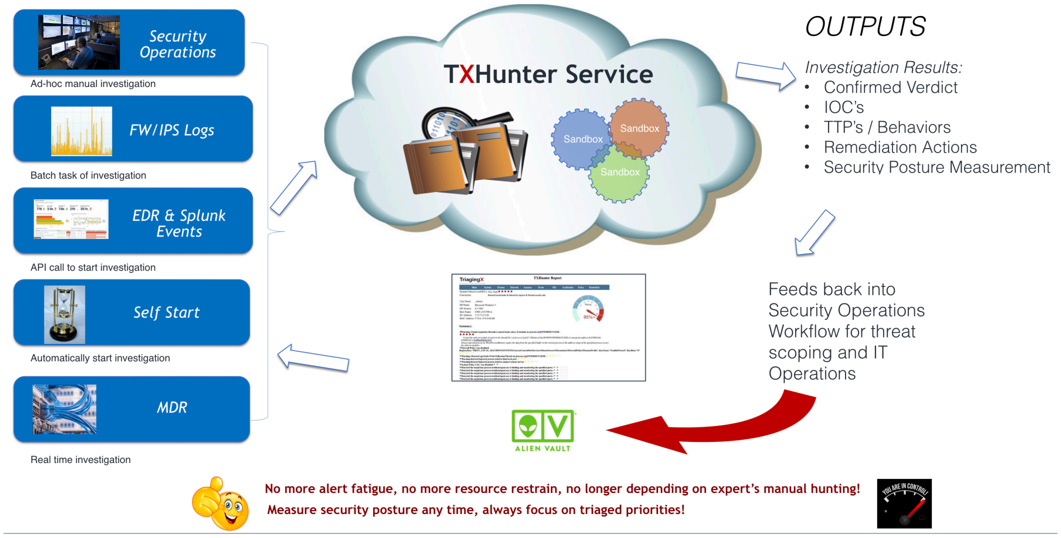
support@triagingx.com

6050 Hellyer Ave
Suite 150-6
San Jose, CA 95138
tel: +1 408.568.7372
support@triagingx.com



TXHunter Has Made Threat Hunting So Easy!

AUTOMATED Endpoint Threat Forensic Investigation



Security Operations

Ad-hoc manual investigation

FW/IPS Logs

Batch task of investigation

EDR & Splunk Events

API call to start investigation

Self Start

Automatically start investigation

MDR

Real time investigation

TXHunter Service

Sandbox

Sandbox

Sandbox

OUTPUTS

Investigation Results:

- Confirmed Verdict
- IOC's
- TTP's / Behaviors
- Remediation Actions
- Security Posture Measurement

Feeds back into Security Operations Workflow for threat scoping and IT Operations

No more alert fatigue, no more resource restrain, no longer depending on expert's manual hunting!

Measure security posture any time, always focus on triaged priorities!

Key Takeaways

TXHunter Benefits

- *No more alert fatigue*
- *Know your security posture and compliance status all time any time*
- *Never need to worry about ransomware attacks*
- *Threat hunting process becomes easy, simple and efficient*
- *No longer lacking of resources and expertise in your team*

TXHunter Automates Endpoint Forensic Threat Hunting Process

- *Fast, only takes 15 minutes or less per investigation*
- *Zero impacts on endpoint system with disposable and light agent*
- *Consistent, always works and delivers the insightful results*
- *Behavior analysis, detects threat that doesn't have documented IOC yet*
- *Exposes potential risks and provides actionable follow ups*

TXHunter Fits Well Into Security Operation Flow

- *Hunting results are in json format, easy to be consumed by all threat management platforms*
- *Its restful APIs and syslog make it easy for integration, already integrated with Cylance & AlienVault & WedgeNetworks MDR, and Splunk*
- *Its flexible employment option works well in cloud and on premises*
- *It automates IR but also works well for baseline monitoring and security posture measurement and proactive threat hunting*

TriagingX Inc.