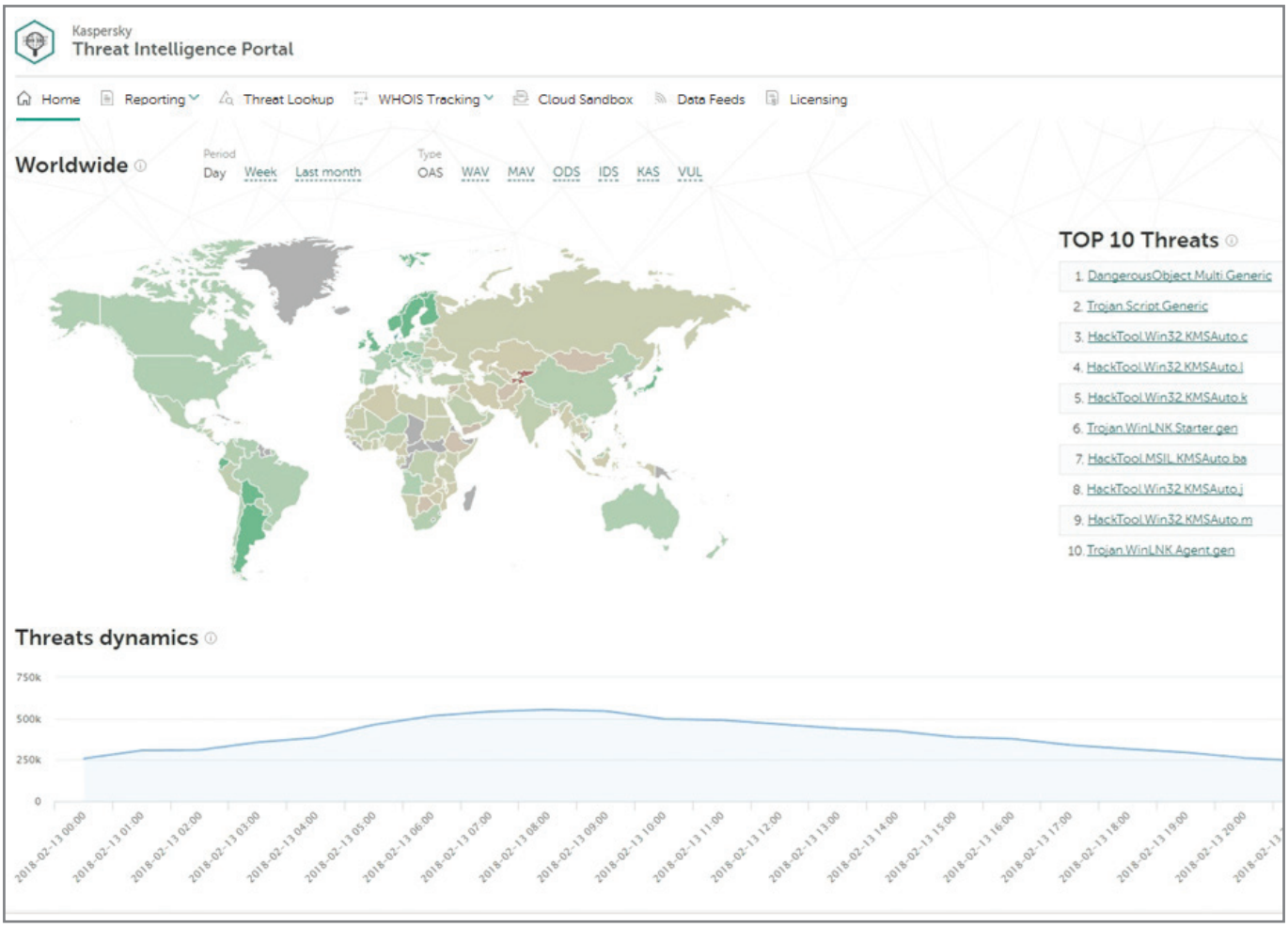
KASPERSKY lab

Portal de inteligência de ameaças da Kaspersky: Investigação e resposta a incidentes

www.kaspersky.com.br/enterprise-security/fraud-prevention
#truecybersecurity

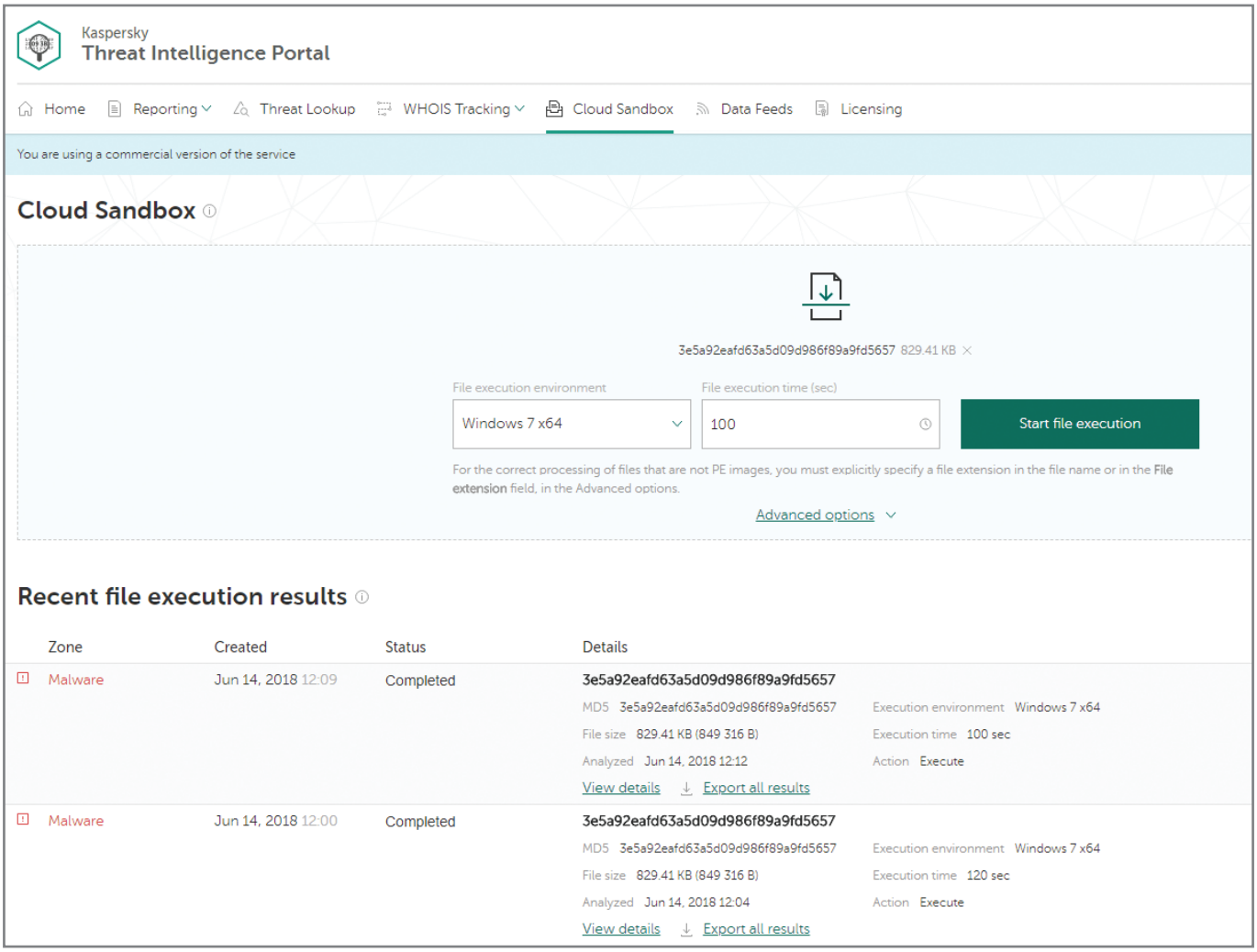
O Portal de inteligência de ameaças da Kaspersky fornece todo o conhecimento que a Kaspersky Lab coletou, aprimorou e categorizou ao longo de mais de 20 anos de história. A plataforma recupera a inteligência de ameaças detalhada mais recente, incluindo arquivos, URLs, domínios, endereços IP, hashes de arquivos, nomes de ameaças, dados estatísticos/comportamentais, dados de WHOIS/DNS, etc., permitindo que os agentes de resposta a incidentes possam:

- Determinar se um evento que está na fila requer uma resposta imediata ou investigação adicional
- Usar a primeira detecção como ponto de partida para averiguar o escopo completo de um incidente e responder de maneira correspondente
- Definir quem foi afetado, o que foi afetado e qual foi o impacto, e fornecer informações significativas para os outros departamentos relevantes
- Entender as táticas e técnicas usadas pelos cibercriminosos, além de seus objetivos, para determinar a resposta mais eficiente

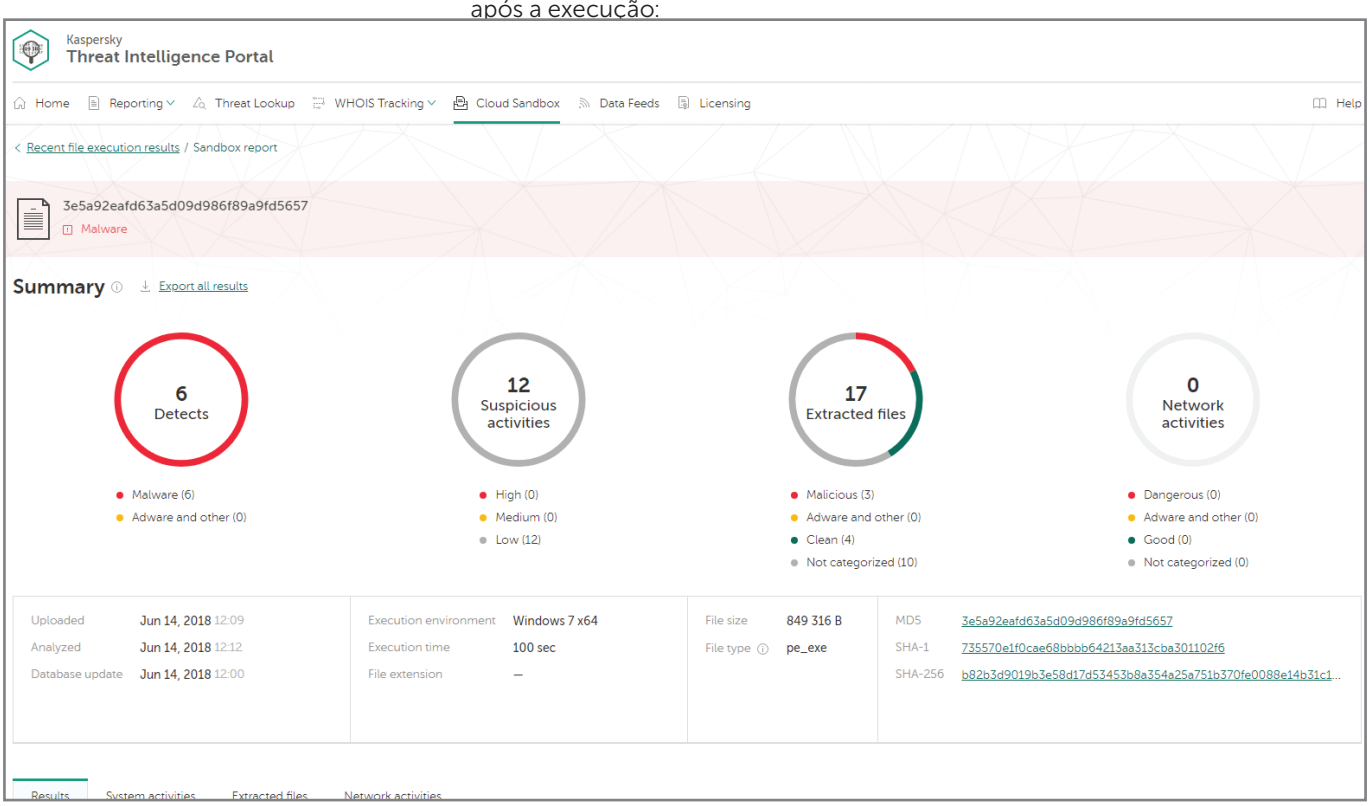


A página principal do Portal de inteligência de ameaças tem várias guias, mas, neste exemplo, vamos imaginar que temos evidências atuais. A equipe de resposta a incidentes obteve uma amostra de arquivo suspeito que iniciou a comunicação de dentro do perímetro da rede com um endereço IP externo, fora do horário de trabalho normal. Então, podemos ir direto para a guia Cloud Sandbox no menu superior.

A Sandbox executa um objeto suspeito em uma máquina virtual (VM) com um sistema operacional com todos os recursos. Ela detecta a atividade maliciosa de um objeto analisando seu comportamento. As VMs são isoladas da infraestrutura real da empresa, então a execução não causará danos reais. Carregue seu arquivo, selecione o ambiente (Windows 7, neste caso), selecione o tempo (vamos tentar 100 segundos) e inicie a execução:



As Sandboxes são eficientes contra malwares que escapam da análise estática; por isso o seu antivírus poderia ignorar totalmente um arquivo suspeito. Mesmo que esse arquivo fosse identificado como "ruim", a maioria dos sistemas antivírus não explicaria seu nível de perigo, nem o que está realmente acontecendo. Para obter mais detalhes, vamos ver o que acontece no Kaspersky Cloud Sandbox após a execução:



Ao executar o objeto testado, a Sandbox coleta artefatos, os analisa e entrega seu veredito. Temos aqui um resumo: detecções (6), atividades suspeitas (12), arquivos extraídos (17) e atividades de rede (0). Não se trata apenas de um arquivo "ruim"; ele realiza muitas coisas prejudiciais, e elas estão todas listadas.

Results | System activities | Extracted files | Network activities

Sandbox detection names

Download data

Zone	Name
High	Trojan.Win32.Pincav.bqeyx
High	HEUR:Trojan.Win32.Generic
High	Trojan.Win32.Gatak.sb
High	Trojan.Win32.Xpun.sb
High	Trojan.Win32.Inject
High	Trojan.Win32.Yakes

Triggered network rules

No data found

Execution map

Suspicious Activity
The file time attributes have been changed

Suspicious Activity
The file time attributes have been changed

Suspicious Activity
Shellcode has been found in process memory

Suspicious Activity
Executable has obtained the privilege

Suspicious Activity
Executable has obtained the privilege

Suspicious activities

Download data

Zone	Severity	Description
Low	290	Shellcode has been found in the memory of the process **$user\$temp\RarSFX0\3086.exe**.
Low	290	The process **$windir\$system32\svchost.exe** has read multiple system files.
Low	290	The file has been created in the system folder
Low	290	The file has been created in the system folder
Low	290	The file has been created in the system folder
Low	290	The file has been created in the system folder
Low	200	The **$windir\$system32\wbem\WmiPrvSE.exe** process has obtained the privilege **SeDebugPrivilege**.
Low	200	The **$windir\$system32\wbem\WmiPrvSE.exe** process has obtained the privilege **SeBackupPrivilege**.
Low	200	The process **$windir\servicing\TrustedInstaller.exe** has run the wildcard search: **$windir\servicing\sqm*.sqm**.
Low	200	The **$windir\servicing\TrustedInstaller.exe** process has obtained the privilege **SeBackupPrivilege**.

Screenshots (20)

Download all

Na guia Results (Resultados), um agente de resposta a incidentes pode ver as capturas de tela feitas durante a execução. Em alguns casos, o malware tenta burlar a análise automática aguardando a interação do usuário (inserção de uma senha, rolagem por um documento, movimentação do mouse, etc.). O Kaspersky Cloud Sandbox conhece muitas técnicas de evasão e usa tecnologias de simulação humana para contê-las. As capturas de tela também podem ser úteis: Um pesquisador pode ver o que está acontecendo no "tubo de ensaio" do ponto de vista humano.

Vamos alternar para a guia Extracted files (Arquivos extraídos) para ver quais objetos foram baixados, extraídos ou removidos. Nesse caso, um arquivo malicioso removido:

Results | System activities | Extracted files | Network activities

Downloaded files

No data found

Dropped files Download data

Zone	MD5	APT	Detection name	File name
Malware	3E5A92EAFD63A5D09D986F89A9FD5657	—	Trojan.Win32.Pincav.bqeyx	3e5a92eafd63a5d09d986f89a9fd5657.exe
Malware	84C212A2E281C8F2EC7783751FC65265	—	—	3086.exe
Malware	DE721AE292DD1EB94F1DA2A2538AAAB2	—	HEUR:Trojan.Win32.Generic	9939.exe

As funcionalidades clássicas da Sandbox parariam por aí: você executou o arquivo e obteve a lista de atividades maliciosas. Pronto. Mas, com o Portal de inteligência de ameaças da Kaspersky, você pode passar diretamente para o Threat Lookup para obter informações mais detalhadas sobre os indicadores de comprometimento e suas relações.

O Threat Lookup é nosso mecanismo de pesquisa de segurança. Ele contém aproximadamente 5 petabytes de inteligência de ameaças, coletada e categorizada pela Kaspersky Lab ao longo dos últimos 20 anos: hashes de arquivos, dados estatísticos/comportamentais, dados de WHOIS/DNS, URLs, endereços IP e assim por diante.

Então, depois que executamos nossa amostra na Sandbox, usamos os resultados obtidos imediatamente para a pesquisa do Threat Lookup; basta clicar no objeto (um hash MD5, neste caso)

Kaspersky
Threat Intelligence Portal

Home | Reporting | Threat Lookup | WHOIS Tracking | Cloud Sandbox | Data Feeds | Licensing

Hash, IP address, domain, or URL

Enter your request here | Look up

More about request types

Hash report for MD5: Malware

Copy request | Export all results

DE721AE292DD1EB94F1DA2A2538AAAB2

Hits	≈ 100	Format	PE	MD5	de721ae292dd1eb94f1da2a2538aaab2
First seen	Jun 04, 2015 16:48	Size	544 768 B	SHA-1	b6bdb2b93f6741854fbc60877b11ba0b9a080a27
Last seen	Aug 10, 2017 10:18	Signed by	None	SHA-256	d7fc75f668aa8450900e4b0995873f073af25b36a064e8b1944a76
		Packed by	None		

Detection names

Jun 05, 2015 03:45
Trojan.Win32.Yakes

Jun 05, 2015 08:44
Trojan.Win32.Yakes.kubx

File signatures and certificates

No data found

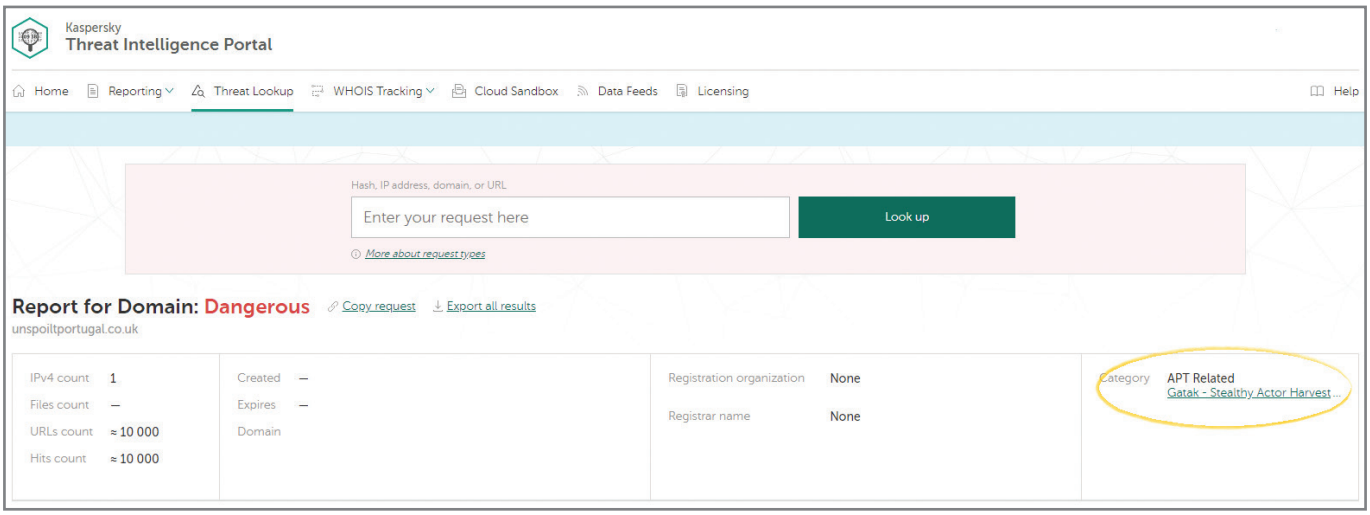
Agora, temos um relatório mais detalhado sobre o malware. Vamos rolar pelos resultados do Threat Lookup para ver quais URLs foram acessados pelo malware que estamos investigando:

File accessed following URLs

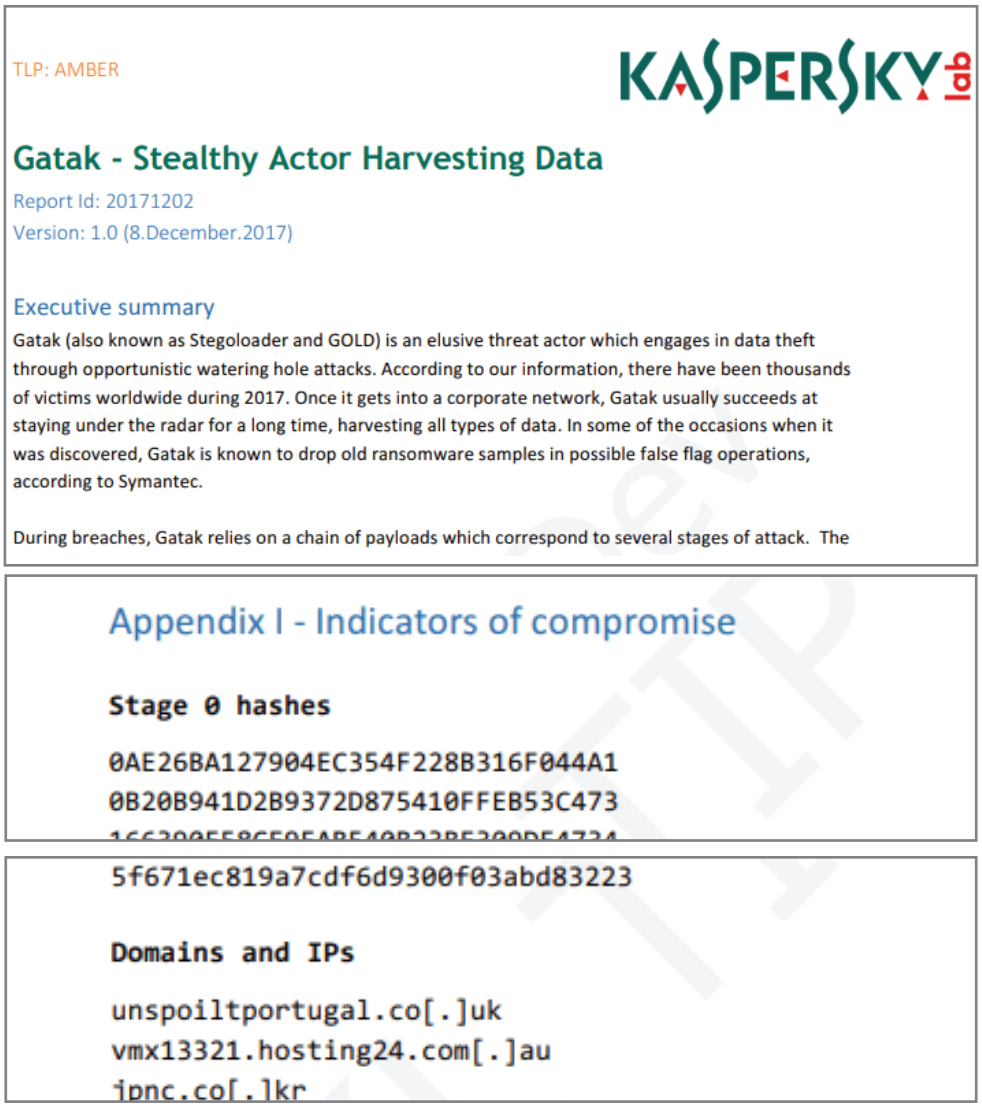
Download data

Status	URL
Dangerous	unspoiltportugal.co.uk/report_N_0027_
Dangerous	unspoiltportugal.co.uk/report_N_0027_9A552DDAC93CC701-B22EF57AF695C501-0000000000000000-00000000
Dangerous	unspoiltportugal.co.uk/report_N_0027_9A552DDAC93CC701-B22EF57AF695C501-0000000000000000-00000000
Dangerous	unspoiltportugal.co.uk/report_N_0027_9A552DDAC93CC701-B22EF57AF695C501-0000000000000000-00000000
Dangerous	unspoiltportugal.co.uk/report_N_0027_9A552DDAC93CC701-B22EF57AF695C501-0000000000000000-00000000
Dangerous	unspoiltportugal.co.uk/report_N_0027_9A552DDAC93CC701-B22EF57AF695C501-0000000000000000-00000000
Dangerous	unspoiltportugal.co.uk/report_N_0027_9A552DDAC93CC701-B22EF57AF695C501-0000000000000000-00000000
Dangerous	unspoiltportugal.co.uk/report_N_0027_9A552DDAC93CC701-B22EF57AF695C501-0000000000000000-00000000
Dangerous	unspoiltportugal.co.uk/report_N_0027_9A552DDAC93CC701-B22EF57AF695C501-0000000000000000-00000000
Dangerous	unspoiltportugal.co.uk/report_N_0027_9A552DDAC93CC701-B22EF57AF695C501-0000000000000000-00000000

Temos aqui um URL marcado como "Dangerous" (Perigoso). Novamente, vamos detalhar esse URL malicioso para ver o que o Threat Lookup sabe sobre ele:



No final, o URL malicioso em questão está relacionado a um ataque de APT! O Portal de inteligência de ameaças da Kaspersky mostra a opção de baixar o relatório da APT. Esse PDF inclui um resumo executivo, detalhes técnicos aprofundados e uma lista dos indicadores de comprometimento relacionados. Vale a pena conferir para ver se aconteceu algo semelhante em sua organização e para desenvolver rapidamente casos de uso específicos para a detecção do ataque descrito.



TLP: AMBER

KASPERSKY lab

Gatak - Stealthy Actor Harvesting Data

Report Id: 20171202
Version: 1.0 (8.December.2017)

Executive summary

Gatak (also known as Stegoloader and GOLD) is an elusive threat actor which engages in data theft through opportunistic watering hole attacks. According to our information, there have been thousands of victims worldwide during 2017. Once it gets into a corporate network, Gatak usually succeeds at staying under the radar for a long time, harvesting all types of data. In some of the occasions when it was discovered, Gatak is known to drop old ransomware samples in possible false flag operations, according to Symantec.

During breaches, Gatak relies on a chain of payloads which correspond to several stages of attack. The

Appendix I - Indicators of compromise

Stage 0 hashes

0AE26BA127904EC354F228B316F044A1
0B20B941D2B9372D875410FFEB53C473

5f671ec819a7cdf6d9300f03abd83223

Domains and IPs

unspoiltportugal.co[.]uk
vmx13321.hosting24.com[.]au
jpnc.co[.]kr

Com o Portal de inteligência de ameaças da Kaspersky, você pode:

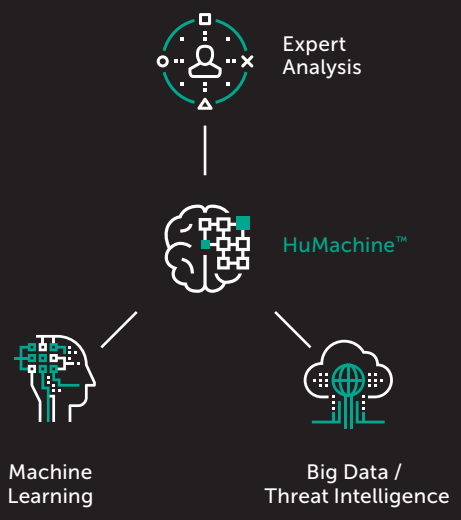
- Melhorar e acelerar os recursos de resposta a incidentes e perícia, fornecendo às equipes de segurança/SOC informações relevantes sobre ameaças e dados globais sobre o que está por trás dos ataques direcionados. Diagnosticar e analisar incidentes de segurança em hosts e na rede com mais eficiência e eficácia, além de priorizar os sinais de sistemas internos contra ameaças desconhecidas, minimizando o tempo de resposta a incidentes e interrompendo a kill chain antes que dados e sistemas críticos sejam comprometidos.

- Fazer pesquisas detalhadas sobre os indicadores de ameaças, como endereços IP, URLs, domínios ou hashes de arquivos, com contexto de ameaças superconfirmado, o que permite priorizar ataques, melhorar as decisões sobre alocação de pessoal e recursos, e se concentrar em atenuar as ameaças que representam mais risco para os seus negócios.

- Atenuar os ataques direcionados. Aprimorar sua infraestrutura de segurança com informações táticas e estratégicas de ameaças, adaptando as estratégias de defesa para combater as ameaças enfrentadas pela sua organização.

Kaspersky Lab
Cibersegurança para empresas: www.kaspersky.com/enterprise
Notícias sobre ameaças cibernéticas: www.securelist.com
Notícias sobre segurança de TI: business.kaspersky.com/

#truecybersecurity
#HuMachine

www.kaspersky.com

© 2019 AO Kaspersky Lab. Todos os direitos reservados. As marcas registradas e marcas de serviço são propriedade dos respectivos titulares.