

BRabbit Lab(mail)

設想

你是一名調查員，受命協助 Drumbo 公司，這家公司最近遭受了勒索軟體攻擊。攻擊始於一名員工收到一封看似來自老闆的電子郵件。郵件中印有公司識別碼和一個熟悉的郵箱地址。該員工誤以為郵件合法，開啟了附件，導致系統被入侵並部署勒索軟體，加密敏感文件。你的任務是調查和分析這些文件，以發現有關攻擊者的信息。

資料風險性提示：

請勿運行此文件，因為它是真正的勒索軟體，可能會對您的系統造成嚴重損害。執行此文件可能會導致您的個人資料被加密，使其無法在不支付贖金的情況下存取。它還可能使攻擊者未經授權控制您的設備，從而可能造成永久性損壞或資料遺失。為了您的安全，請勿與此文件互動並立即將其刪除。如果您必須分析它，請僅在安全、隔離的環境（例如虛擬機器）中進行。

密碼：感染

問題 1

用於傳遞惡意附件的網路釣魚郵件顯示多項潛在社會工程攻擊跡象。識別這些跡像有助於識別未來類似的威脅。

發送該附件的可疑電子郵件地址是什麼？

使用工具：<https://eml-analyzer.herokuapp.com/#/>

EML Analyzer

HomeCacheAPIGitHub

Cache

Headers

Basic headers

Message ID	<1419576.bWFhcmtrbm9wZmxlckBnbWFpbC5jb20=@iobBeE5>
Subject	Immediate Action Required: Your Employment Contract.
Date (UTC)	2024-12-13T22:27:38Z
From	theceojamesmith@drurnbo.com
To	rafael@drumbo.com

theceojamesmith@Drurnbo.com

第二季

該勒索軟體被識別為已知惡意軟體家族的一部分。確定其家族名稱可以深入了解其行為和補救策略。調查中發現的勒索軟體的家族名稱是什麼？

Attachments

#1

Filename	Urgent Contract Action.pdf.exe
Size	431.5 Kb
MIME type	PE32 executable (console) Intel 80386, for MS Windows, 5 sections
SHA256	630325cac09ac3fab908f903e3b00d0dadd5fdaa0875ed8496fcb97a558d0da

- Copy to clipboard
- AnyRun
- Hybrid Analysis
- InQuest
- VirusTotal

630325cac09ac3fab908f903e3b00d0dadd5fdaa0875ed8496fcb97a558d0da

Community Score -1528

peexe calls-wmi overlay checks-user-input executes-dropped-file checks-disk-space signed direct-cpu-clock-access long-sleep detect-debug-environment checks-network-adapters attachment invalid-signature service-scan checks-cpu-name runtime-modules

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY 30+

Join our Community

and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Popular threat label

trojan.badrabbit/diskcoder

Threat categories

trojan ransomware worm

Family labels

badrabbit diskcoder

badrabbit

第三季

勒索軟體執行後，會將一個檔案投放到受感染的系統上，以啟動其有效載荷。識別該文件對於理解其感染過程至關重要。

勒索軟體投放的第一個檔案叫什麼名字？

Attachments

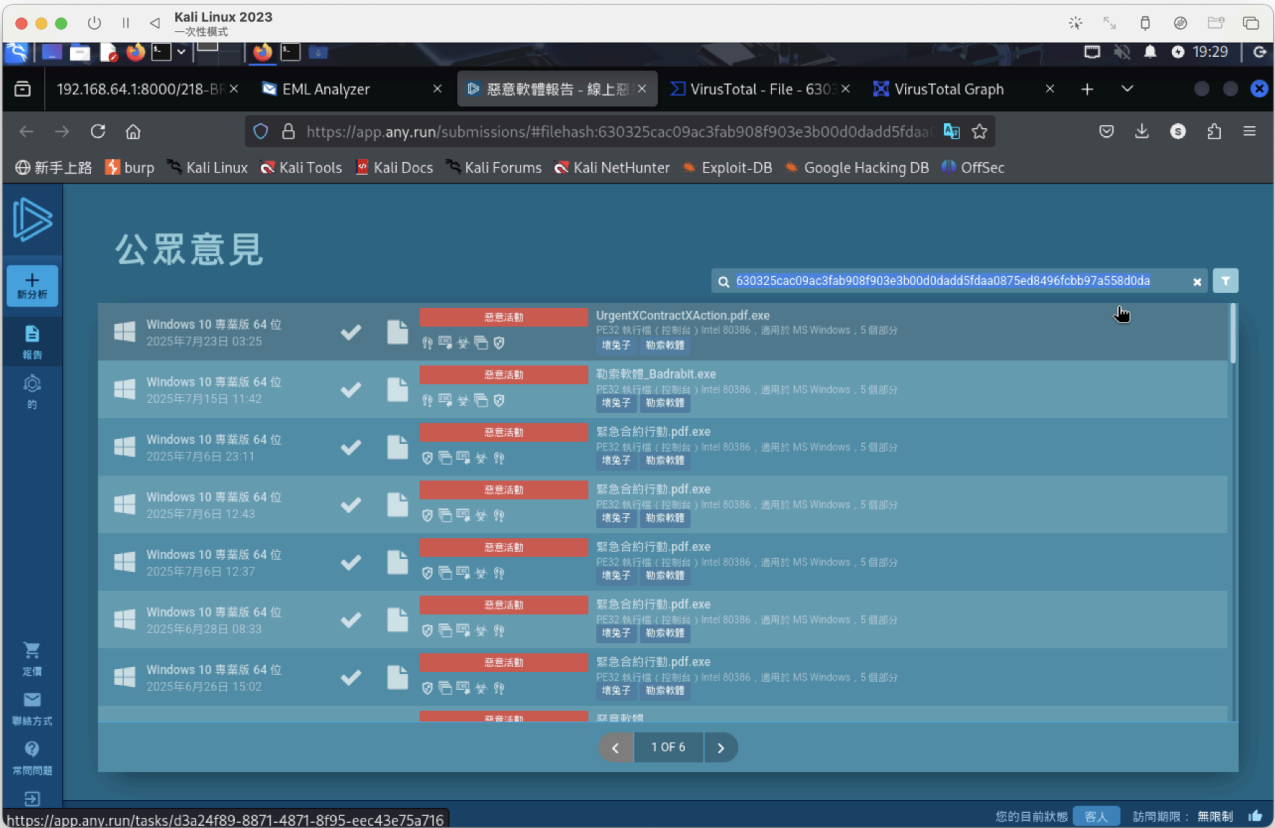
#1

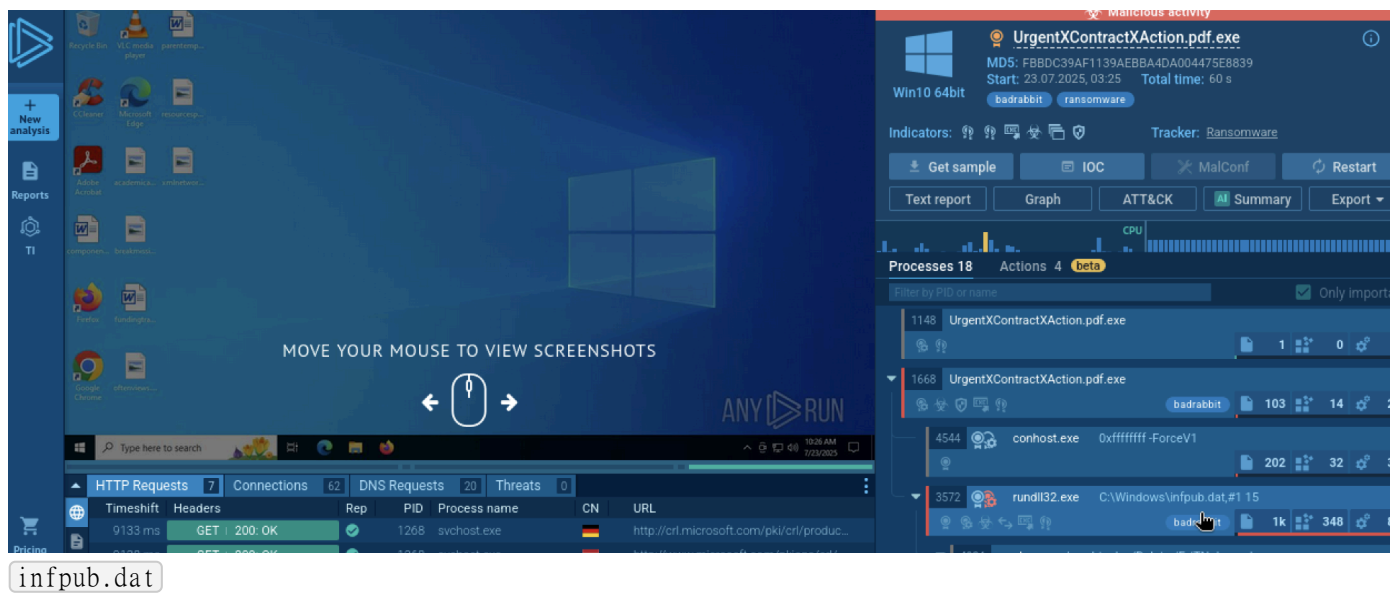
Filename	Urgent Contract Action.pdf.exe
Size	431.5 Kb
MIME type	PE32 executable (console) Intel 80386, for MS Windows, 5 sections
SHA256	630325cac09ac3fab908f903e3b00d0dadd5fdaa0875ed8496fcb97a558d0da

Copy to clipboard

AnyRun

輸入sha256





第四季

在被植入的文件中，惡意軟體包含硬編碼訊息，包括使用者名稱和密碼，這些資訊可能提供有關其來源或配置的線索。

在被植入的檔案中，唯一找到的使用者名稱是什麼？

Google搜尋：badrabbit infpub.dat username list

參考網站：<https://www.f-secure.com/v-descs/trojan-w32-rabbad.shtml>

Products ▾ Renew Articles ▾ Support Free tools ▾ Scam protection My F-Secure

■ Motherboard: New ransomware - Bad Rabbit - Spreading Quickly Through Russia and Ukraine

Infection

From our analysis, the initial infection vector for the Bad Rabbit ransomware is via compromised websites that host an injected malicious script. The script redirects users to a secondary site where the actual ransomware file is downloaded. The actual file itself may be disguised as an Adobe Flash Player update.

Bad Rabbit also includes functionality to spread through a network, as it is able to check for accessible SMB shares using hardcoded usernames and passwords:

Username

■ Administrator	■ ftp	■ asus
■ Admin	■ rdp	■ ftpuser
■ Guest	■ rdpuser	■ ftpadmin
■ User	■ rdpadmin	■ nas
■ User1	■ manager	■ nasuser
■ user-1	■ support	■ nasadmin
■ Test	■ work	■ superuser
■ root	■ other user	■ netguest
■ buh	■ operator	■ alex
■ boss	■ backup	

問5

勒索軟體執行後會與 C2 伺服器通訊。了解其通訊技術有助於緩解威脅。MITRE ATT&CK 的哪個子技術描述了該勒索軟體如何使用 Web 協定發送和接收資料？

Command and Control TA0011		
Uncommonly Used Port T1065		
Severity	Description	Match
INFO	Tries to connect to UDP port 137 at 72.247.153.178.	-
Application Layer Protocol T1071		
Severity	Description	Match
INFO	Uses HTTPS	HTTP traffic on port 49694 -> 443 HTTP traffic on port 49680 -> 443

家 > 科技 > 企業 > 應用層協定 > Web協定

應用層協定：Web協定

應用層協定其他子技術 (5)

攻擊者可能會使用與網路流量相關的應用層協定進行通信，透過混入現有流量來規避偵測/網路過濾。發送到遠端系統的命令，以及這些命令的結果，通常會嵌入在客戶端和伺服器之間的協定流量中。

諸如 HTTP/S^[1]和 WebSocket^[2]之類的承載網路流量的協定在實際環境中可能非常常見。HTTP/S 封包包含許多欄位和標頭，資料可能隱藏在其中。攻擊者可能會濫用這些協定與受害網路中受其控制的系統進行通信，同時也能模仿正常的預期流量。

編號： T1071.001

T1071的子技術

- ① 戰術： 指揮與控制
- ① 平台： ESXi、Linux、網路設備、Windows、macOS
- 貢獻者： TruKno
- 版本： 1.4
- 創建日期： 2020年3月15日
- 最後修改日期： 2025年4月15日

[版本永久連結](#)

例子

T1071.001

問6

持久性機制是複雜勒索軟體的標誌。識別持久性機制的實現方式有助於恢復並防止再次感染。與勒索軟體持久性技術關聯的 MITRE ATT&CK 子技術 ID 是什麼？

技術細節

了解此威脅的含義

子技術

T1053.005

“計劃任務”

所需權限： 行政人員

資料來源： Windows 登錄： Windows 登錄項目創建， 文件： 文件修改， 文件： 文件創建， 流程： 流程創建， 命令： 命令執行， 網路流量： 網路流量， 計劃作業： 計劃作業創建

攻擊者可能會濫用 Windows 任務排程器來執行任務調度，以便首次或重複執行惡意程式碼。Windows 中有多種方法可以存取任務排程器。可以直接在命令列中執行schtasks實用程序，也可以透過控制面板中「管理員工具」部分的 GUI 開啟任務計劃程序。（參考：Stack Overflow）在某些情況下，攻擊者會使用 Windows 工作排程器的 NET 包裝

● 此進程透過任務計劃程序執行 (1)

6488 更新程式.exe (1)

● 使用任務計劃程式運行其他應用程式 (2)

4648 cmd.exe (1)

3888 命令提示 字元(1)

影像：

C:\Windows\SysWOW64\schtasks.exe

命令列：

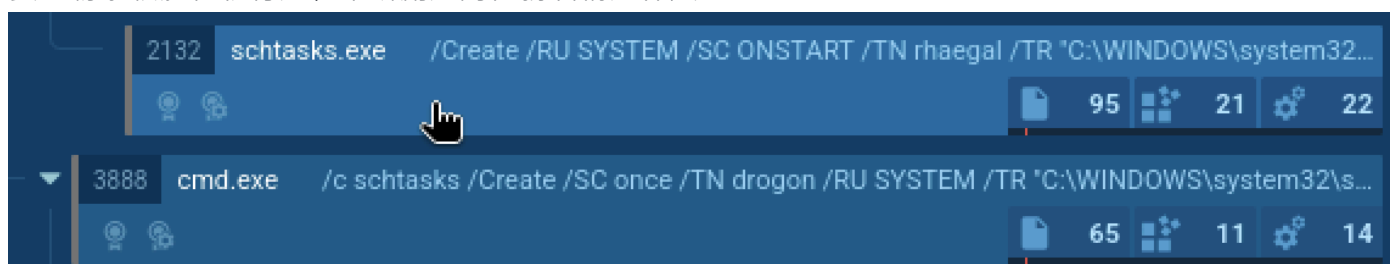
schtasks /Create /SC once /TN drogon /RU SYSTEM /TR "C:\WINDOWS\system32\shutdown.exe /r /t 0 /f" /ST 10:43:00

◀ 1 共 1 ▶

T1053.005

問7

作為感染鏈的一部分，勒索軟體創建了特定的任務以確保其持續運作。識別這些任務對於系統恢復至關重要。勒索軟體在執行過程中所創造的任務名稱是什麼？



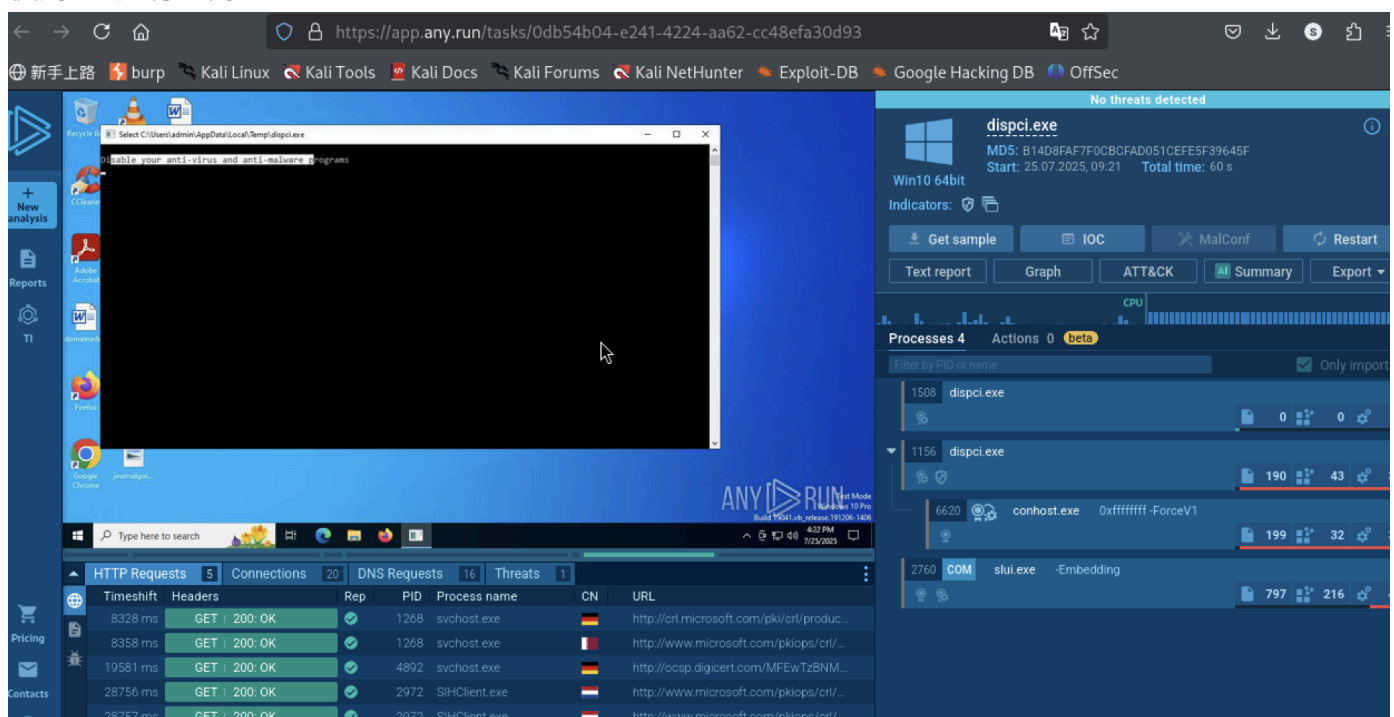
rhaegal,drogon

問8

該惡意二進位檔案在執行時dispci.exe會顯示一條可疑訊息，敦促使用者停用防禦措施。此策略旨在逃避偵測，並使勒索軟體能夠完全執行。執行此二進位檔案時，控制台中顯示了哪些可疑訊息？



使用sha進行查詢




Disable your anti-virus and anti-malware programs

問9

為了修改主開機記錄 (MBR) 並加密受害者的硬碟，勒索軟體使用了一個特定的驅動程式。識別該驅動程式對於理解加密機制至關重要。

用於加密硬碟和修改 MBR 的驅動程式叫什麼名字？



8ebc97e05c8e1073bda2efb6f4d00ad7e789260afa2c276f0c72740b838a0a93

File Version Information


Copyright	http://diskcryptor.net/
Product	GrayWorm
Description	Microsoft Display Class Installer
Original Name	dispci.exe
File Version	1.1.846.118

diskcryptor

Q10

歸因是了解威脅情勢的關鍵。勒索軟體透過其策略、技術和程序 (TTP) 與一個已知的攻擊組織聯繫在一起。

負責這次勒索軟體活動的威脅行為者是誰？



Inventory Statistics Usage ApiVector Login

BadRabbit

 EternalPetya aka. ExPetr, Pnyetya, Petna, NotPetya, Nyetya, NonPetya, nPetya, Diskcoder.C, BadRabbit

win.eternal_petya (Back to overview)

 **EternalPetya**

Propose Change

aka: ExPetr, Pnyetya, Petna, NotPetya, Nyetya, NonPetya, nPetya, Diskcoder.C, BadRabbit

Actor(s): TeleBots, Sandworm

 VTCollection

According to proofpoint Bad Rabbit is a strain of ransomware that first appeared in 2017 and is a suspected variant of Petya. Like other strains of

Sandworm

問11

該勒索軟體透過破壞關鍵系統組件，導致系統無法啟動。識別所使用的技術可以深入了解其破壞能力。用於破壞系統韌體並阻止啟動的技術的 MITRE ATT&CK ID 是什麼？

<https://attack.mitre.org/software/S0606/>

企業	T1495	韌體損壞	Bad Rabbit使用了一個可執行檔來安裝已修改的引導程序，以阻止正常啟動。 ^[1]
----	-------	------	--

T1495