新型惡意軟體 Kobalos 攻擊活動及相關技術分析

總頁數，：13 頁（含封面及附件）

文件編號：X-101

機密等級：□機密□密■一般

©數聯資安股份有限公司

中華民國 110 年 02 月 05 日

目錄

壹、 相關訊息 3

貳、 訊息深入探討 4

一、 Kobalos 介紹 5

二、 Kobalos 後門介紹 6

三、 配合 Kobalos 使用的 SSH 竊取程式 7

四、 Kobalos 如何隱藏 7

五、 結語 9

參、 防護及修補建議 10

肆、 Indicatorsofcompromise(IoCs) 11

伍、 參考資料 12

圖 目 錄

圖 1 ESET 原文連結 4
圖 2 bleepingcomputer 原文連結 4
圖 3 ESET 掃描出受感染的世界範圍地圖 5
圖 4 Kobalos 後門功能概述和操作方式 6
圖 5 Kobalos 的流程控制圖 7
圖 6 概述 Kobalos 網絡協議的序列圖 8

壹、 相關訊息

ESET 發表了一篇文章，內容為其研究人員發現新型惡意軟體 Kobalos 的攻擊活動並加以分析，Kobalos 的程式源碼僅有 24KB，相較於其他惡意軟體更為嬌小但更加複雜並能在跨 Unix、AIX 和 Windows 系統上執行。

ESET 研究人員針對惡意軟體樣本特徵進行全世界網路掃描，已發現到許多學術和研究領域的超級電腦或伺服器受感染。

貳、 訊息深入探討

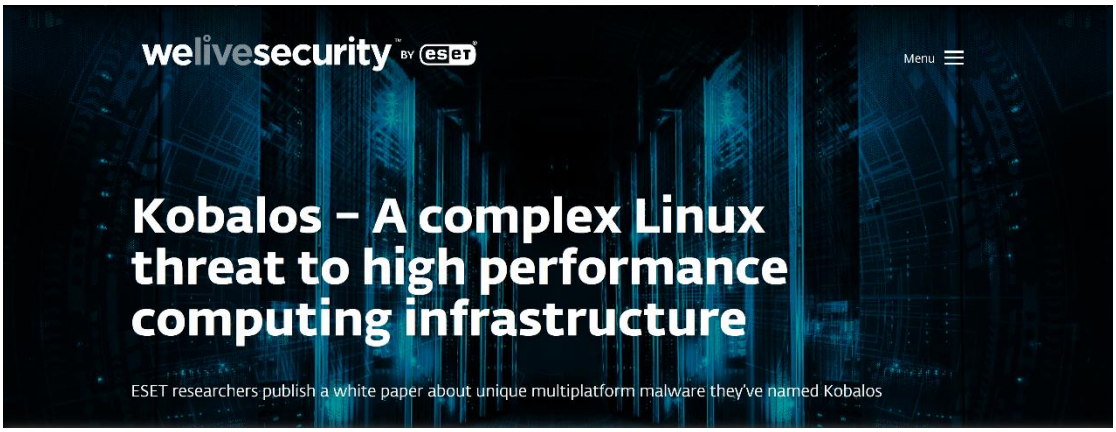
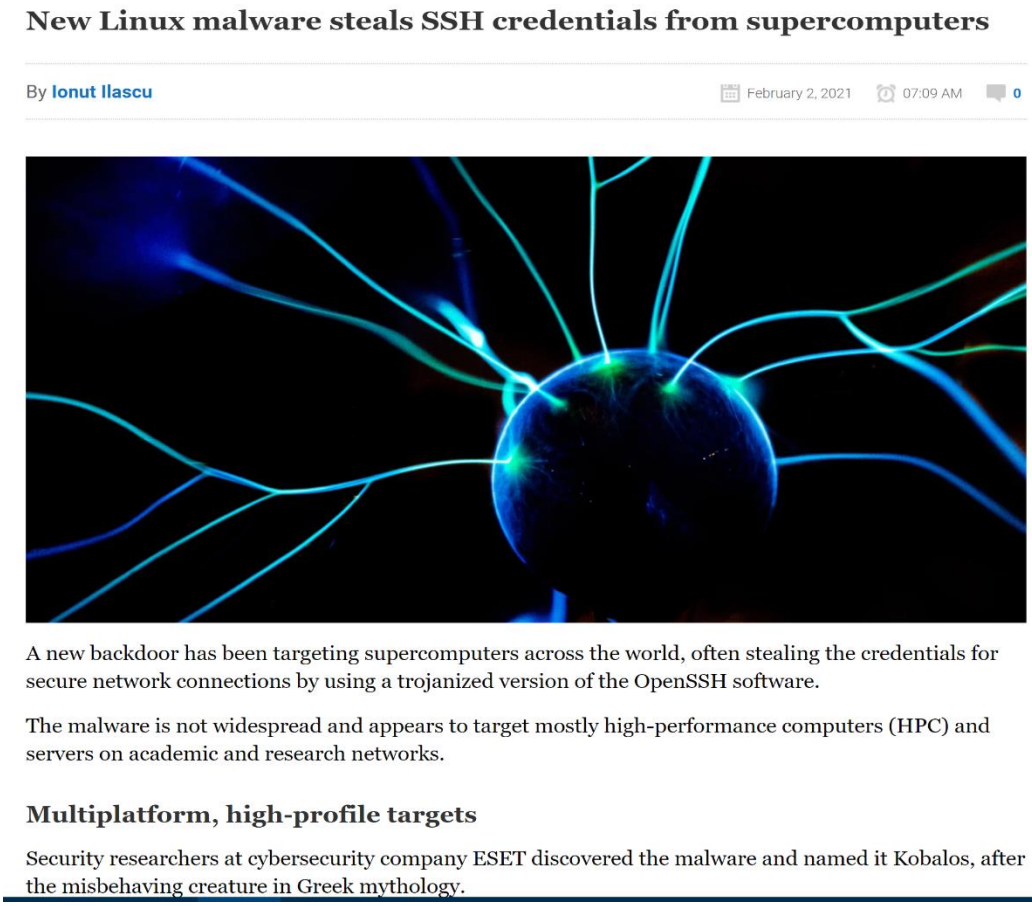


圖1　*ESET 原文連結*



New Linux malware steals SSH credentials from supercomputers

By Ionut Ilascu　February 2, 2021　07:09 AM　0

A new backdoor has been targeting supercomputers across the world, often stealing the credentials for secure network connections by using a trojanized version of the OpenSSH software.

The malware is not widespread and appears to target mostly high-performance computers (HPC) and servers on academic and research networks.

Multiplatform, high-profile targets

Security researchers at cybersecurity company ESET discovered the malware and named it Kobalos, after the misbehaving creature in Greek mythology.

圖2　*bleepingcomputer 原文連結*

一、 Kobalos 介紹

ESET 發表了一篇文章，內容為其研究人員發現新型惡意軟體 Kobalos 的攻擊活動並加以分析，Kobalos 的程式源碼僅有 24KB，相較於其他惡意軟體更為嬌小但更加複雜並能在跨 Unix、AIX 和 Windows 系統上執行。

ESET 研究人員針對惡意軟體樣本特徵進行全世界網路掃描，已發現到許多學術和研究領域的超級電腦或伺服器受感染。

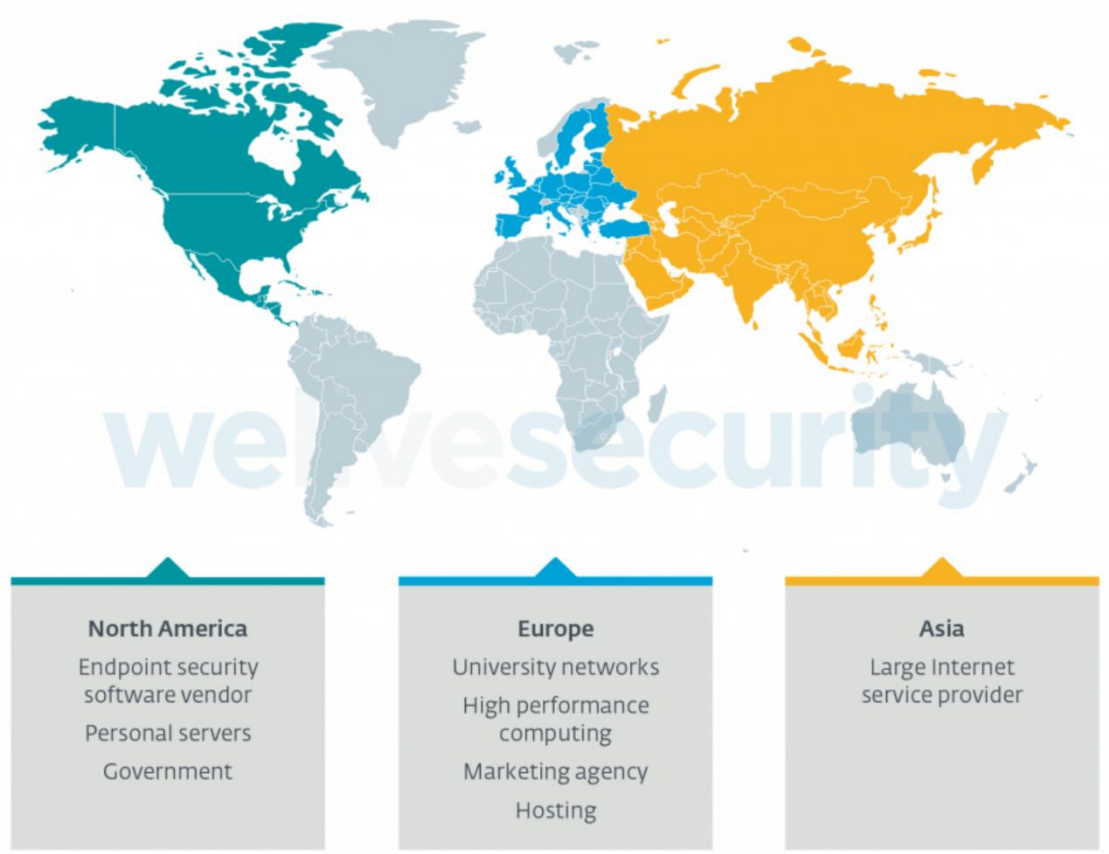


圖3　*ESET 掃描出受感染的世界範圍地圖*

二、 Kobalos 後門介紹

Kobalos 相較於其他惡意軟體後門，功能極為簡單僅有對文件系統的遠端存取權限、指令終端等功能，並允許 Proxy 與其他受 Kobalos 感染伺服器連接。

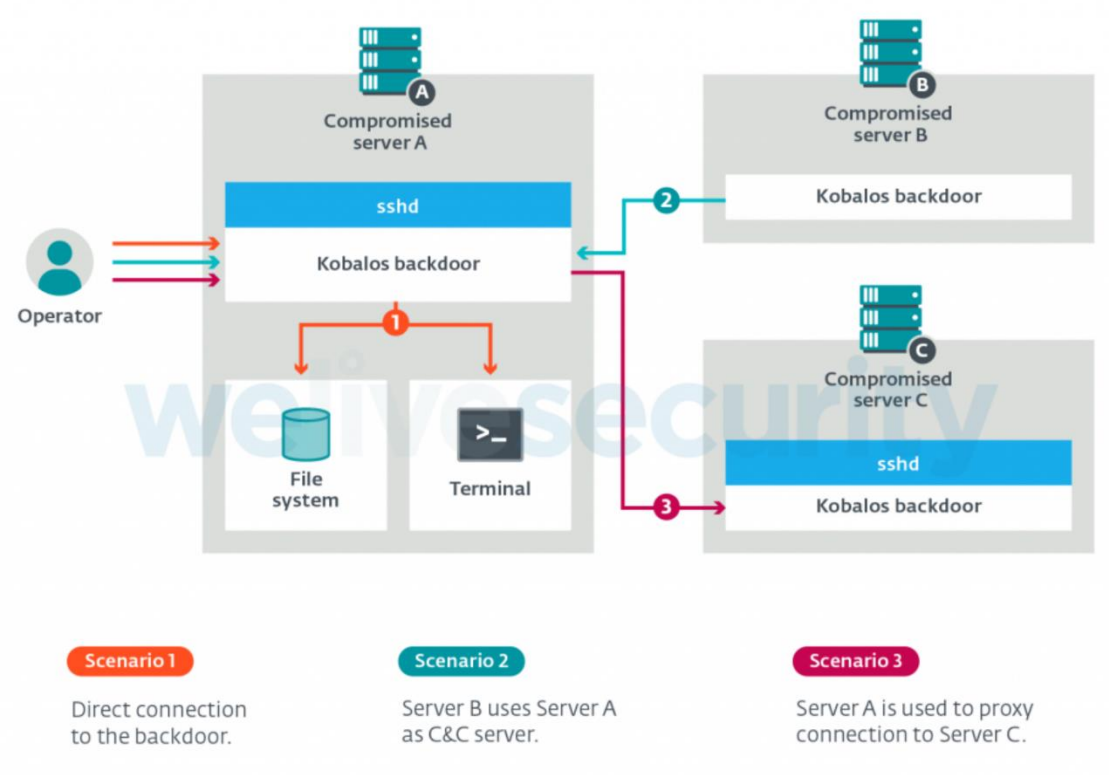


圖4　*Kobalos 後門功能概述和操作方式*

攻擊者有多種方法可以操作受 Kobalos 感染的主機，最常見的方法是將 Kobalos 嵌入 OpenSSH 的 sshd 中，或是使用未被 Kobalos 嵌入 sshd 的變體，連接到將充當 C&C 伺服器。

Kobalos 獨特之處在於 C&C 伺服器的程式碼就在 Kobalos 內，透過攻擊者發送單個指令，任何遭 Kobalos 植入的伺服器都可以轉變為 C&C 伺服器。

三、 配合 Kobalos 使用的 SSH 竊取程式

根據研究人員的觀察，被 Kobalos 植入的大多數系統中的 SSH 客戶端都已被破壞並竊取帳密。此帳密竊取程式的執行方式不同於過去常見的手段。字串未加密、僅將被盜的帳秘寫入硬碟內文件。

此帳密竊取程式的存在可能代表 Kobalos 的傳播方式，使用受感染主機的 SSH 客戶端的任何人都能捕獲其帳密。然後攻擊者可以使用這些帳密在新發現的伺服器上安裝 Kobalos。

四、 Kobalos 如何隱藏

分析 Kobalos 並不像大多數 Linux 惡意軟體那樣麻煩，因為它的所有程式碼都保存在一個函數中，該函數透過遞迴調用自身來執行子任務。

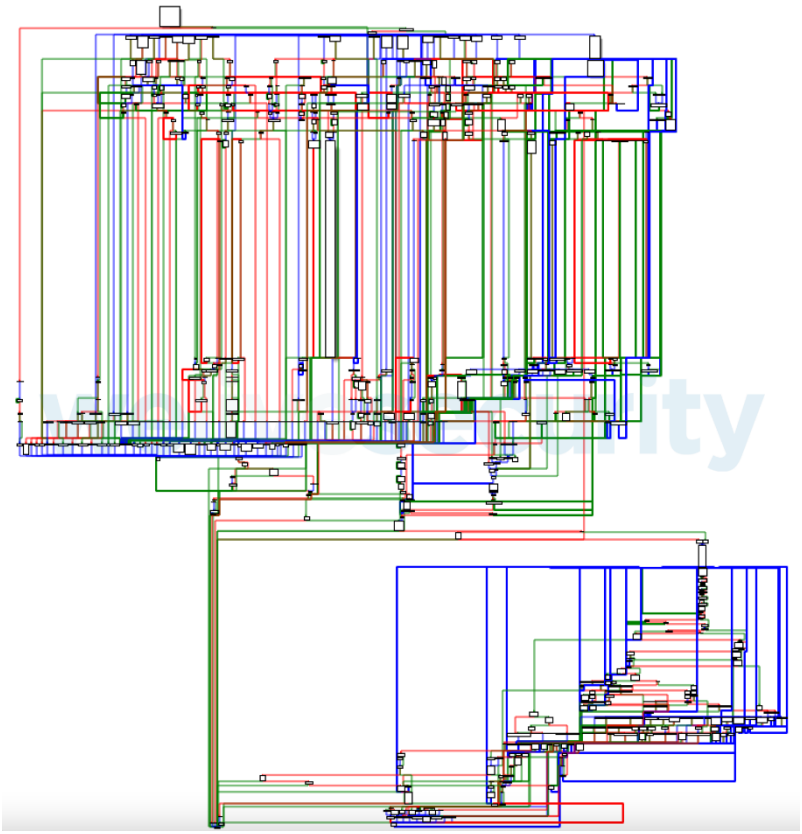


圖5　*Kobalos 的流程控制圖*

這使得分析更具挑戰性，同時所有相關字串皆已被加密，因此與靜態查看樣本相比，動態分析查看惡意程式碼更加困難。

Kobalos 使用後門需要一個 512 bit 的 RSA 私鑰和一個 32 字元長的密碼，一旦通過身份驗證，便會交換 RC4 密鑰並用它們加密其餘的通訊，如下圖所示。

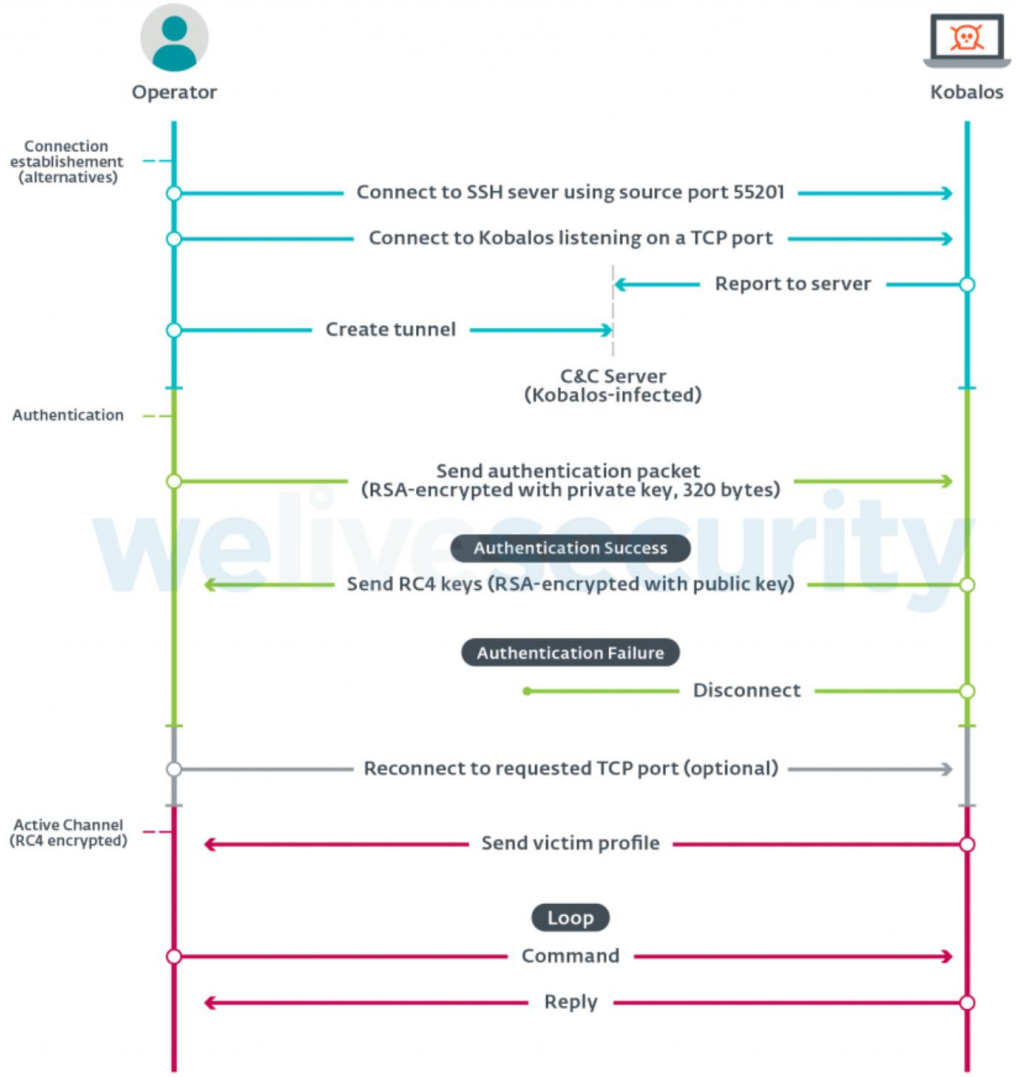


圖6　*概述 Kobalos 網絡協議的序列圖*

五、 結語

研究人員無法確定 Kobalos 背後的駭客組織的意圖，在受感染主機上並沒有發現其他惡意軟體，將 Kobalos 緊密地包含在單個功能中的方式以及使用現有開放端口來訪問 Kobalos 的方式使這種威脅更難找到。

這種複雜性在 Linux 惡意軟體中很少見，考慮到它比平均水平還更加先進並且損害了相當多的企業組織，因此 Kobalos 可能會持續存在一段時間。

參、 防護及修補建議

分類	簡單介紹及針對此 IOC 可以執行的防護操作
IP Address	建議將對應的 IP 透過防火牆、IPS 規則或是黑名單來進行阻擋或是限制存取。
SHA1	此為惡意程式、病毒、惡意文件等檔案以不同的演算法經過內容換算得出來的 HASH，用以辨識不同的樣本，建議透過防毒軟體的 CUSTOM HASH BANNING 進行手動增加已使對應樣本能被貴客戶所使用之防護設備偵測並阻擋。

肆、 Indicatorsofcompromise(IoCs)

- IP Address
  - 151[.]80.57.191

- SHA1
  - fbf0a76ced2939d1f7ec5f9ea58c5a294207f7fe
  - 479f470e83f9a5b66363fba5547fdfcf727949da
  - affa12cc94578d63a8b178ae19f6601d5c8bb224
  - 325f24e8f5d56db43d6914d9234c08c888cdae50
  - a4050a8171b0fa3ae9031e0f8b7272facf04a3aa
  - 6616de799b5105ee2eb83bbe25c7f4433420dff7
  - e094dd02cc954b6104791925e0d1880782b046cf
  - 1dd0edc5744d63a731db8c3b42efbd09d91fed78
  - c1f530d3c189b9a74dbe02cfeb29f38be8ca41ba
  - 659cbdf9288137937bb71146b6f722ffcda1c5fe

伍、參考資料

- https://www.bleepingcomputer.com/news/security/new-linux-malware-steals-ssh-credentials-from-supercomputers/
- https://www.welivesecurity.com/2021/02/02/kobalos-complex-linux-threat-high-performance-computing-infrastructure/