Kobalos – A complex Linux threat to high performance computing infrastructure

welivesecurity.com/2021/02/02/kobalos-complex-linux-threat-high-performance-computing-infrastructure/

February 2, 2021

ESET researchers publish a white paper about unique multiplatform malware they've named Kobalos

ESET researchers have analyzed malware that has been targeting high performance computing (HPC) clusters, among other high-profile targets. We reverse engineered this small, yet complex, malware that is portable to many operating systems including Linux, BSD, Solaris, and possibly AIX and Windows. We have named this malware Kobalos for its tiny code size and many tricks; in Greek mythology, a Kobalos is a small, mischievous creature. Today we publish a paper titled "A wild Kobalos appears: Tricksy Linux malware goes after HPCs" describing the inner working of this threat.

A wild Kobalos appears: Tricksy Linux malware goes after HPCs

Download Research Paper

Perhaps unrelated to the events involving Kobalos, there were multiple security incidents involving HPC clusters in the past year. Some of them hit the press and details were made public in an advisory from the European Grid Infrastructure (EGI) CSIRT about cases where cryptocurrency miners were deployed. The EGI CSIRT advisory shows compromised servers in Poland, Canada and China were used in these attacks. Press articles also mention Archer, a breached UK-based supercomputer where SSH credentials were stolen, but do not contain details about which malware was used, if any.

We've worked with the CERN Computer Security Team and other organizations involved in mitigating attacks on scientific research networks. According to them, the usage of the Kobalos malware predates the other incidents. While we know Kobalos compromised large HPC clusters, no one could link the Kobalos incidents to the use of cryptocurrency malware. The malware and the techniques described in these other attacks are different. We also know Kobalos is not exclusively targeting HPCs: we found that a large Asian ISP, a North American endpoint security vendor (not us), as well as some personal servers were also compromised by this threat.

Tiny code, big targets

Thorough analysis of Kobalos revealed that it is sometimes possible to remotely determine if a system is compromised by connecting to the SSH server using a specific TCP *source* port. Using that knowledge, ESET researchers scanned the internet to find potential victims. We were able to identify multiple targets of Kobalos, including HPC systems.

Figure 1. Industry and region of compromised organizations

We notified all identified victims and worked with them to remediate.

The backdoor

Kobalos is a generic backdoor in the sense that it contains broad commands that don't reveal the intent of the attackers. In short, Kobalos grants remote access to the file system, provides the ability to spawn terminal sessions, and allows proxying connections to other Kobalos-infected servers.

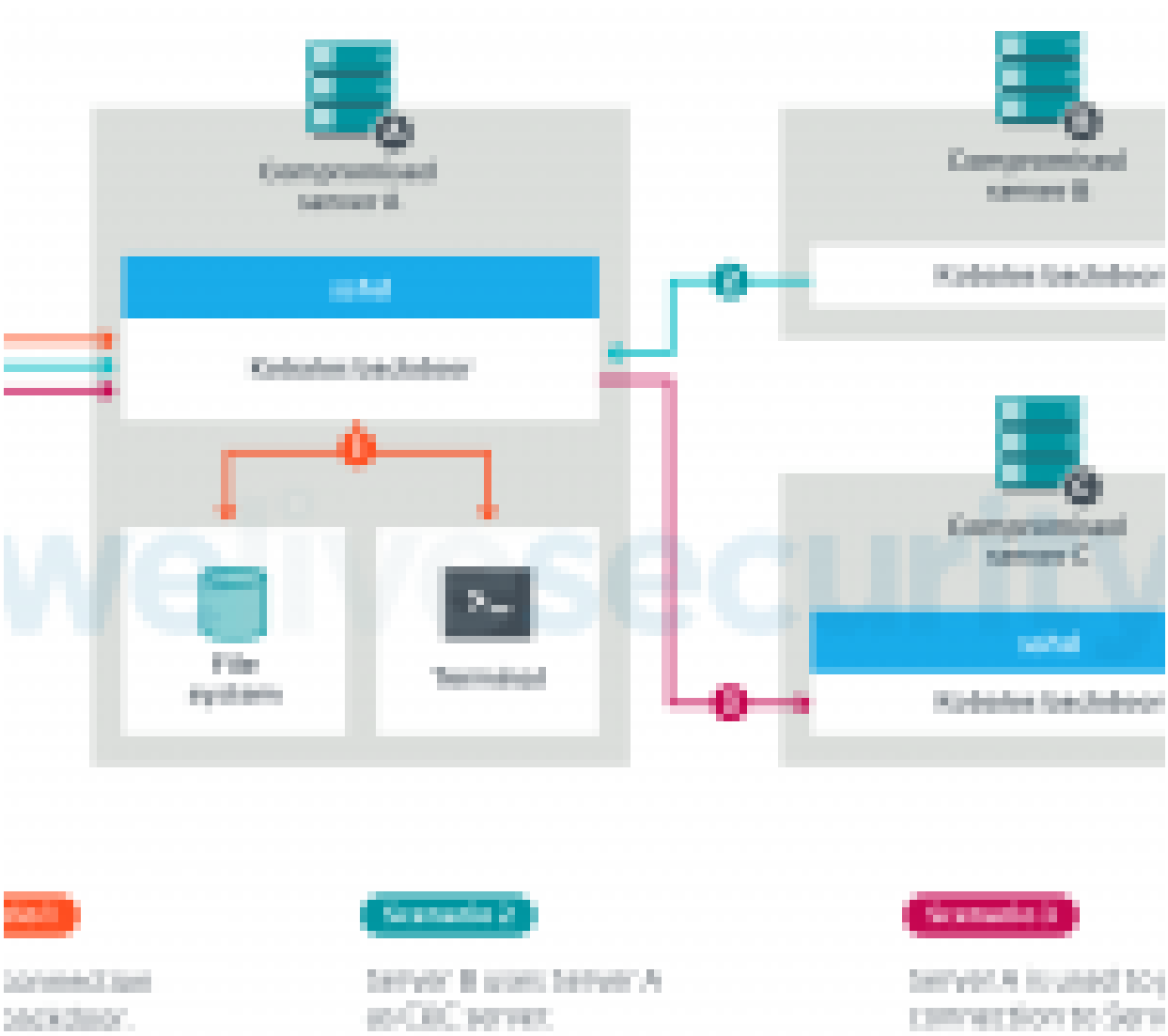

Figure 2. Overview of Kobalos features and ways to access them

There are multiple ways for the operators to reach a Kobalos-infected machine. The method we've seen the most is where Kobalos is embedded in the OpenSSH server executable (sshd) and will trigger the backdoor code if the connection is coming from a specific TCP source port. There are other stand-alone variants that are not embedded in sshd. These variants either connect to a C&C server that will act as a middleman, or wait for an inbound connection on a given TCP port.

Something that makes Kobalos unique is the fact that the code for running a C&C server is in Kobalos itself. Any server compromised by Kobalos can be turned into a C&C server by the operators sending a single command. As the C&C server IP addresses and ports are hardcoded into the executable, the operators can then generate new Kobalos samples that use this new C&C server.

The sidekick

In most systems compromised by Kobalos, the SSH client is compromised to steal credentials. This credential stealer is unlike any of the malicious OpenSSH clients we've seen before, and we've looked at tens of them in the past eight years. The sophistication of this component is not the same as Kobalos itself: there was no effort to obfuscate early variants of the credential stealer. For example, strings were left unencrypted and stolen usernames and passwords are simply written to a file on disk. However, we found newer variants that contain some obfuscation and the ability to exfiltrate credentials over the network.

The presence of this credential stealer may partially answer how Kobalos propagates. Anyone using the SSH client of a compromised machine will have their credentials captured. Those credentials can then be used by the attackers to install Kobalos on the newly discovered server later.

How it hides

Analyzing Kobalos isn't as trivial as most Linux malware because all of its code is held in a single function that recursively calls itself to perform subtasks.

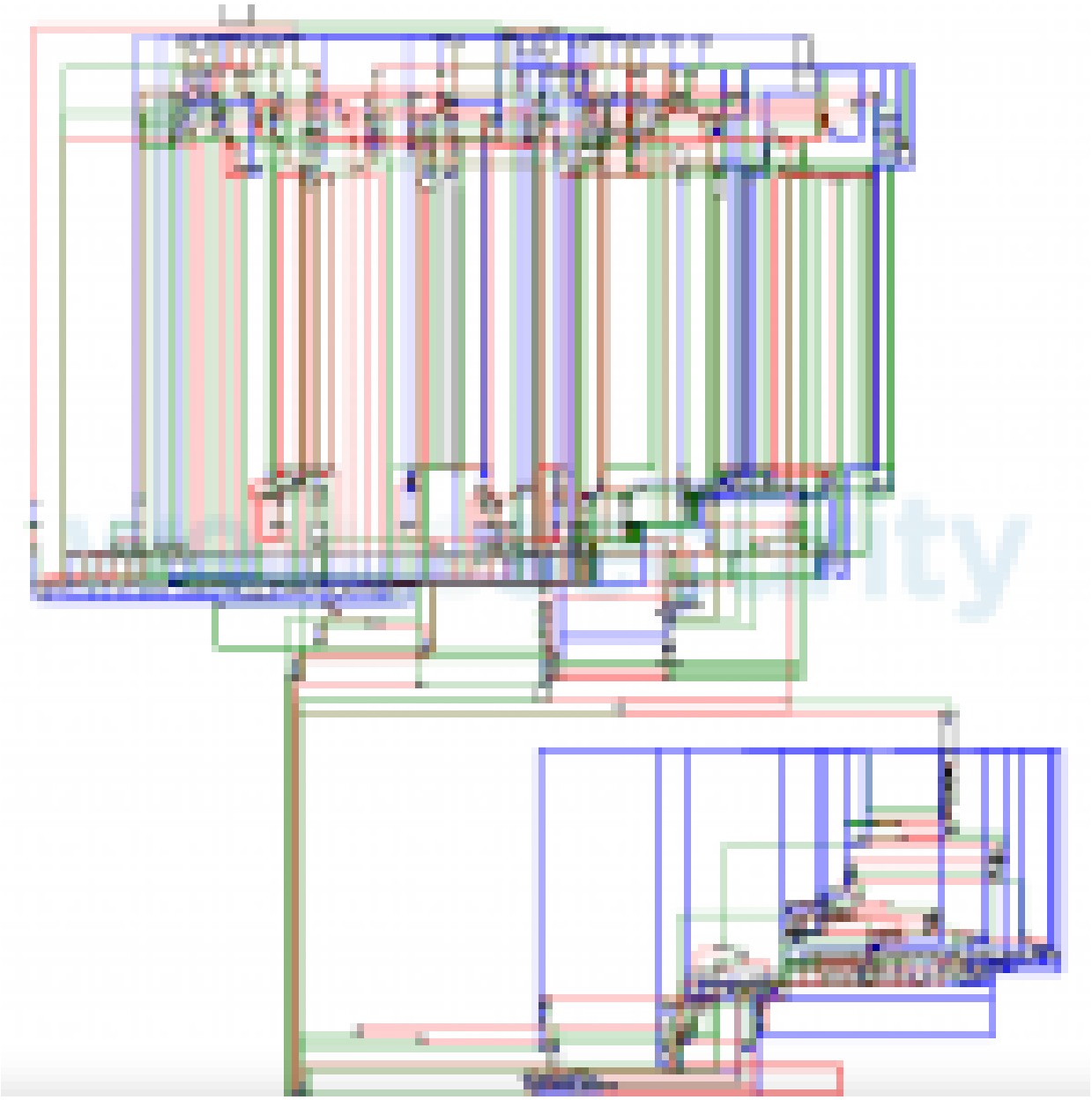

Figure 3. Control flow graph of Kobalos

This makes it more challenging to analyze. Additionally, all strings are encrypted so it's more difficult to find the malicious code than when looking at the samples statically.

Usage of the backdoor requires a private 512-bit RSA key and a 32-byte-long password. Once authenticated, RC4 keys are exchanged and the rest of the communication is encrypted with them.

The network protocol is summarized by the sequence diagram.

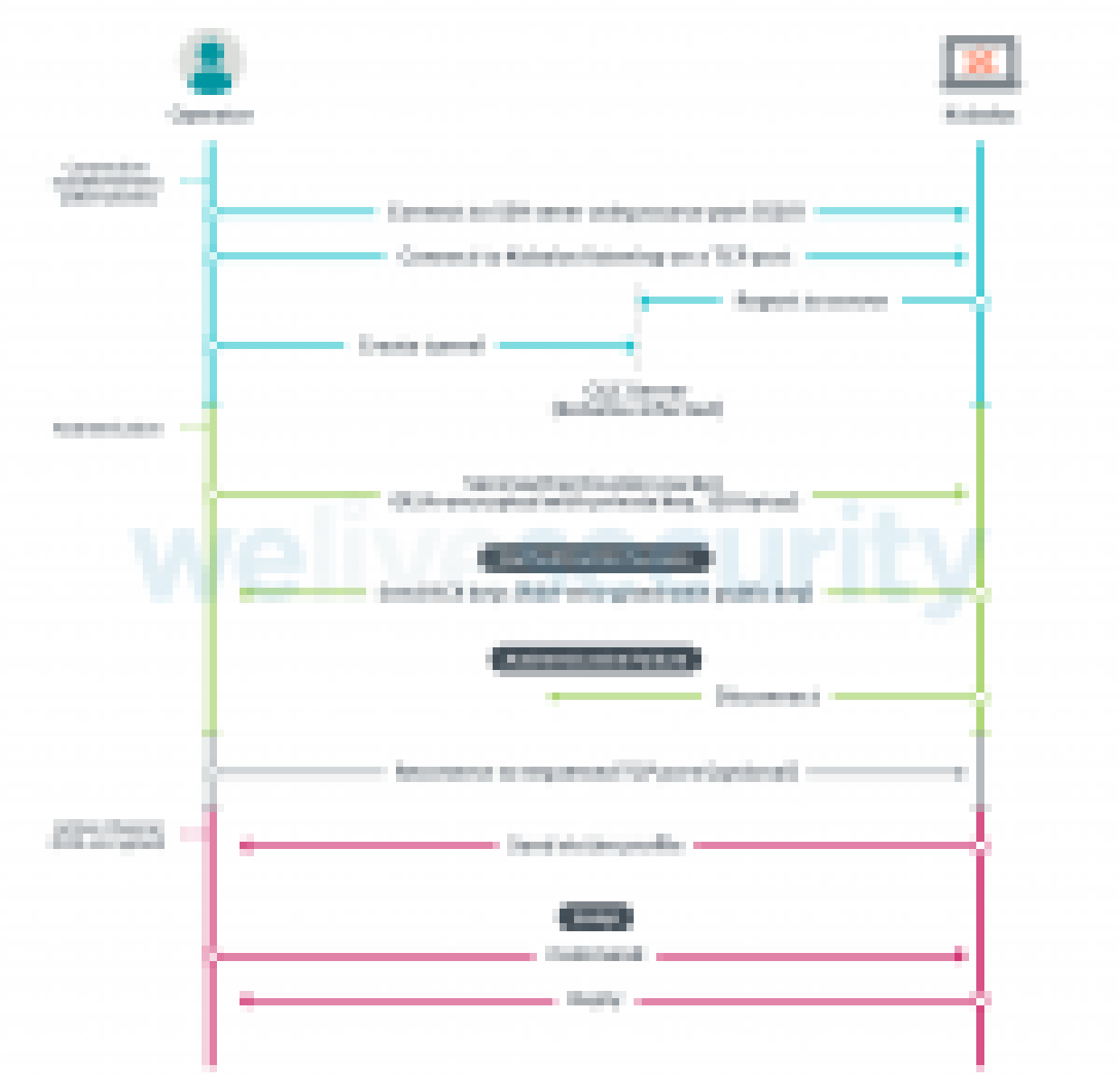

Figure 4. Sequence diagram summarizing Kobalos network protocols

Remediation

ESET products detect the Kobalos malware as Linux/Kobalos or Linux/Agent.IV. The SSH credential stealer is detected as Linux/SSHDoor.EV, Linux/SSHDoor.FB or Linux/SSHDoor.FC. A YARA rule is also available in ESET's malware-ioc repository on GitHub.

From a network perspective, it is possible to detect Kobalos by looking for non-SSH traffic on the port attributed to an SSH server. When the Kobalos backdoor communicates with an operator, there is no SSH banner (SSH-2.0-…) exchanged, neither from the client nor the server.

We have suggested before setting up two-factor authentication (2FA) for connecting to SSH servers. Kobalos is another case where 2FA could have mitigated the threat, since the use of stolen credentials seems to be one of the ways it is able to propagate to different systems.

Conclusion

We were unable to determine the intentions of the operators of Kobalos. No other malware, except for the SSH credential stealer, was found by the system administrators of the compromised machines. We also didn't have access to network traffic captures of the operators in action.

The way Kobalos is tightly contained in a single function and the usage of an existing open port to reach Kobalos makes this threat harder to find. Hopefully the details we reveal today in our new publication will help raise awareness around this threat and put its activity under the microscope. This level of sophistication is only rarely seen in Linux malware. Given that it's more advanced than the average and that it compromised rather large organizations, Kobalos may be running around for a little while.

A comprehensive list of Indicators of Compromise (IoCs) and samples can be found in our GitHub repository.

For any inquiries, or to make sample submissions related to the subject, contact us at threatintel@eset.com.

We would like to acknowledge the work of Maciej Kotowicz from MalwareLab.pl who also analyzed Kobalos independently and with whom we mutually share results. He presented on this threat at the Oh My H@ck 2020 conference.

MITRE ATT&CK techniques

This table was built using version 8 of the ATT&CK framework.

Tactic	ID	Name	Description
Persistence	T1554	Compromise Client Software Binary	Kobalos may embed its malicious payload in the OpenSSH server and replace the legitimate file (sshd). Kobalos replaces the SSH client on compromised systems to steal credentials.

Tactic	ID	Name	Description
T1205	Traffic Signaling	Kobalos may be triggered by an incoming TCP connection to a legitimate service from a specific source port.	
Defense Evasion	T1070.003	Clear Command History	No command history related to the attack was found on Kobalos-infected machines.
T1070.006	Timestomp	When files are replaced by Kobalos operators, timestamps are forged.	
T1027.002	Software Packing	Kobalos's code is flattened into a single function using a custom packer and its strings are encrypted.	
Command and Control	T1573.001	Encrypted Channel: Symmetric Cryptography	Kobalos's post-authentication communication channel is encrypted with RC4.
T1573.002	Encrypted Channel: Asymmetric Cryptography	Kobalos's authentication and key exchange is performed using RSA-512.	
T1090.003	Proxy: Multi-hop Proxy	Kobalos can serve as a proxy to other Kobalos-compromised systems.	

2 Feb 2021 - 11:30AM

Discussion