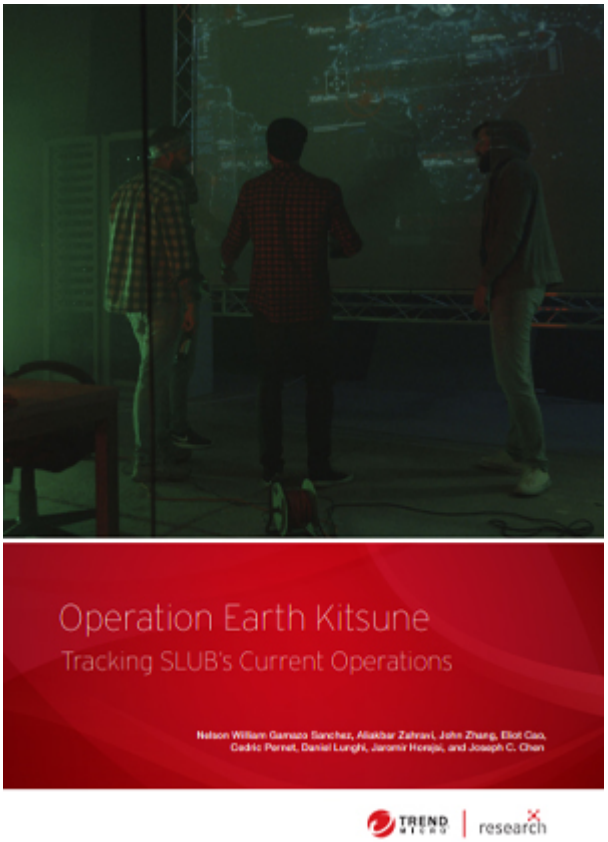
Operation Earth Kitsune: Tracking SLUB’s Current Operations

Archived: 2026-04-05 15:13:51 UTC

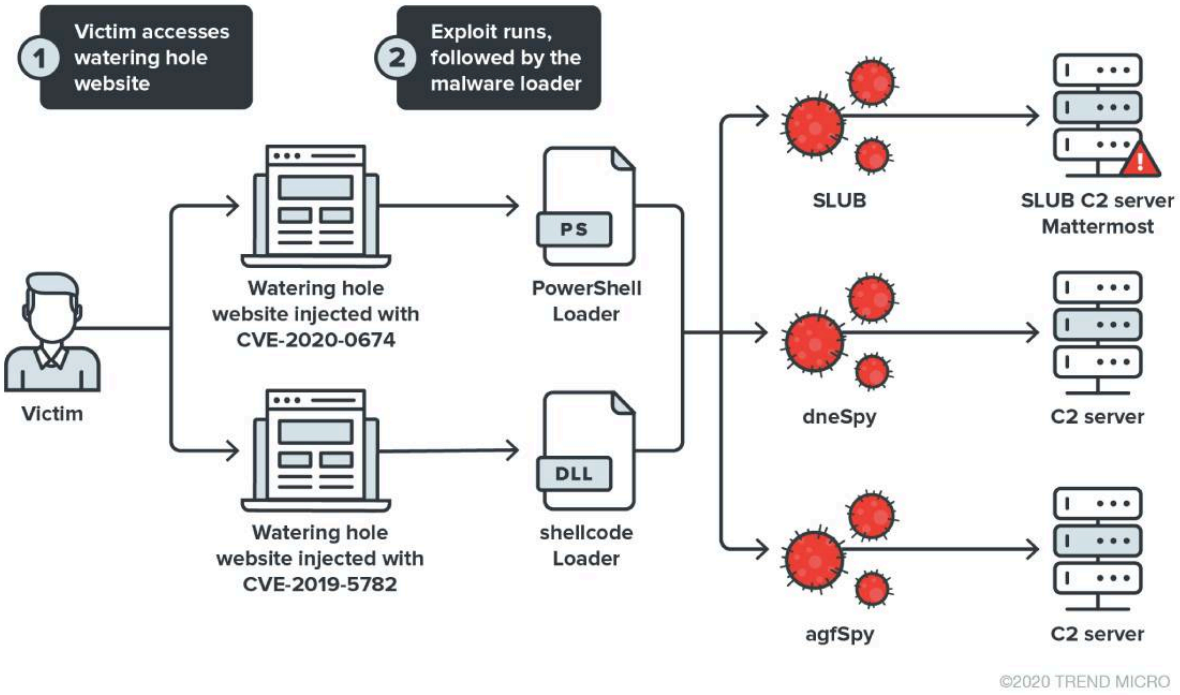


open on a new tabDownload Operation Earth Kitsune: Tracking SLUB’s Current Operations

We have already published findings on the SLUB malware’s past campaigns. In our latest research paperopen on a new tab, we uncovered a recent watering hole campaign that involves a new variant of the malware. The threat, which we dubbed as such due to its abuse of Slack and GitHub in previous versions, has not abused either of the platforms this time; instead, it employed Mattermost, an open-source online chat service that can be easily deployed on-premise.

In an official statement regarding the issue, Mattermost denounced illicit and unethical use of their platform, as this is a definite violation of their Conditions of Useopen on a new tab policy. They also shared how users can report illicit use of the softwareopen on a new tab.

We found Operation Earth Kitsune using a total of five C&C servers, seven samples, and four new bugs, aiming to compromise websites to host malware. We initiated our investigation after noticing that the Korean American National Coordinating Council (KANCC) website was redirecting visitors to the Hanseattle website. Users who accessed the said site were redirected to a weaponized version of a proof of concept (POC) for the CVE-2019-5782open on a new tab Google Chrome vulnerability published in the chromium tracking systemopen on a new tab. Digging deeper, we discovered that the attack does not only involve a weaponized version of the mentioned Chrome exploit; the exploit was infecting the victim machine with three separate malware samples.



open on a new tab

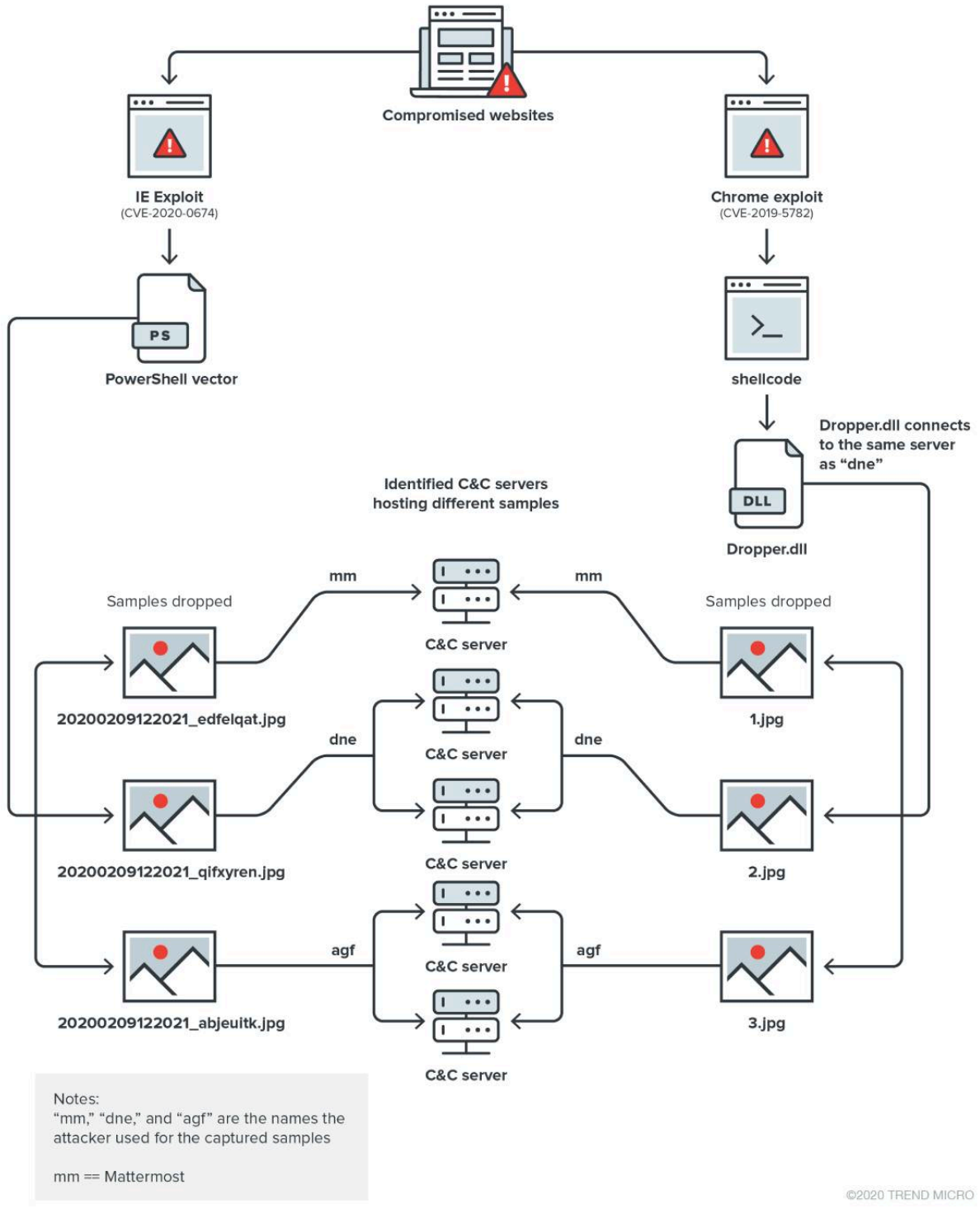
Figure 1. The campaign's infection chain

CVE-2020-0674open on a new tab, a vulnerability in Internet Explorer, was also used to compromise websites. While a shellcode was used for the Chrome exploit, a PowerShell loader was used in the Internet Explorer exploit. Both the samples delivered by the shellcode and PowerShell script connect to the same C&C servers.

Besides the aforementioned behavior, the campaign was also seen exploiting other vulnerabilities, such as CVE-2016-0189open on a new tab, CVE-2019-1458open on a new tab, and the vulnerabilities cited in our previous reports on SLUB.

Like the aforementioned affected sites, the compromised servers are using the GNUBoard Content Management System (CMS), some of them on either version 4 or version 5.

Besides SLUB, two new malware variants, which we dubbed dneSpy and agfSpy, are also linked to this campaign. While SLUB's objective in this campaign is to exfiltrate system information, the two other malware variants were deployed to gain additional control of the affected user’s machine. We believe that the operators of SLUB also released these malware variants. We are currently investigating these samples and will share any pertinent findings.



open on a new tab

Figure 2. The attack vectors used in the campaign

The Chrome Attack Vector

For the Chrome attack vector, the exploit used CVE-2019-5782 and another vulnerability that does not have an assigned CVE. To deploy a weaponized version of this, the attacker reused a POC code. It also implemented two

customizations: the separation of the shellcode to load in from the Javascript encoded version, and the inclusion of support for other operating system versions.

The shellcode requests the dropper.dll from the network; after deobfuscation, it loads the DLL payload address space of the running process.

Dropper.dll checks the system for installed antimalware products by comparing the current processes to a predefined list. If none are detected, the dropper will start downloading three samples, namely “1.jpg,” “2.jpg,” and “3.jpg.”

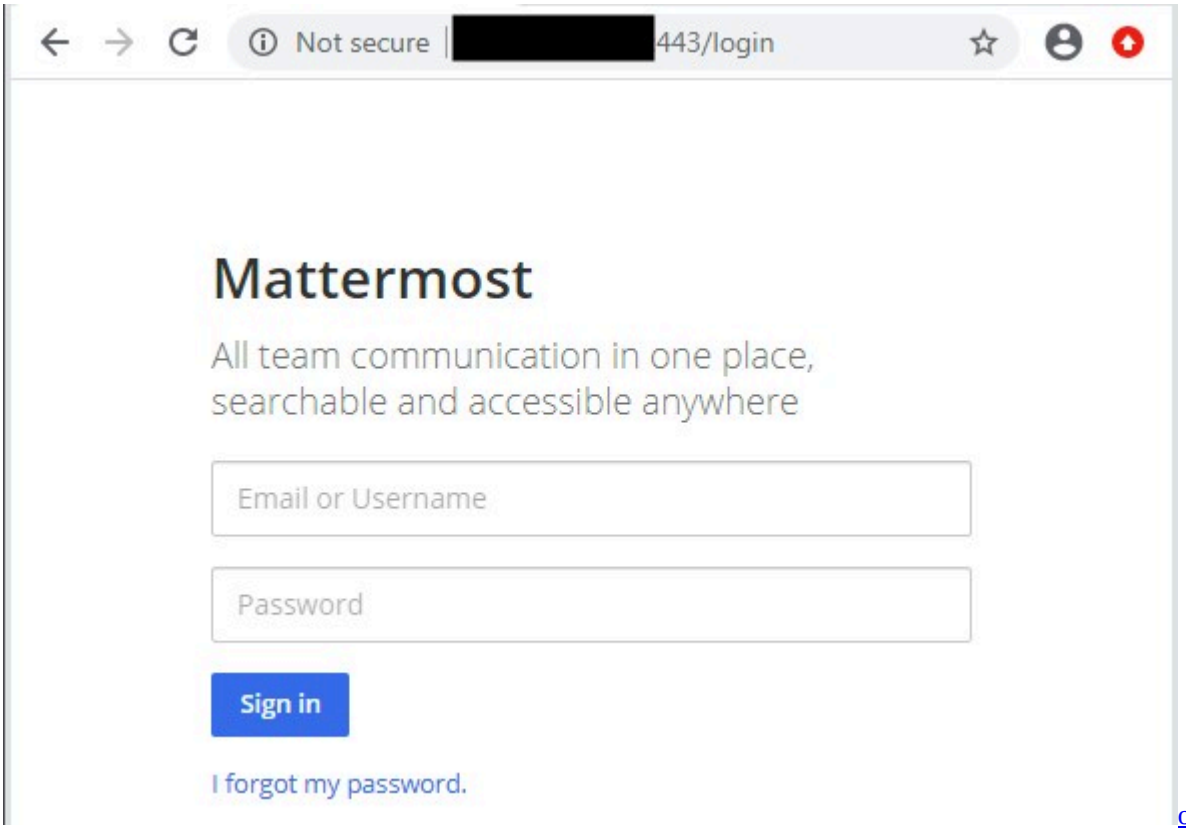
The Internet Explorer attack vector

For the infection vector that uses the Internet Explorer exploit CVE-2020-0674, the exploit runs a shellcode, which executes a few stages of a PowerShell loader.

Similar to the shellcode used in the Chrome exploit chain, the PowerShell version checks if the affected system has any antimalware product installed. If none are installed, the PowerShell proceeds to download and execute three backdoors. If instructed in the LPE (Local Privilege Escalation) column, the PowerShell loader may also initiate the download and execution of an LPE binary exploiting CVE-2019-1458.

SLUB's Use of Mattermost

The SLUB variant used in this campaign employs Mattermost to keep track of its deployment by creating a channel for each infected machine. All communication uses HTTP in port 443.



open on a new tab

Figure 3. Mattermost server operating on port 443.

The malware's communication with Mattermost requires an authentication token that can grant permissions for certain functions such as creating channels and sending posts to these channels.

To learn more about the attacker's infrastructure, we reviewed Mattermost's API. Eventually, we were able to collect the following information:

- The list of channels.
- The dump of all posts in each channel.
- The dump of all screenshots in each channel.
- The list of all users associated with the channels.

The actual list of users showed that the server was first set up on March 10, 2020. It also gave us an insight into the roles each user plays and the kind of permissions they have; "system_admin" for the admin user, and "system_user_access_token" and "system_post_all_public" for regular users.

id	created_datetime	username	email	roles
54ojpfrfdp8qfchn8xom37885r	3/10/2020 6:48	eidkcmrufjvn		system_user system_admin
5z1dengfntrq7rxzspjj54djqa	3/12/2020 0:32	sdkfljaljkfh		system_user system_user_access_token system_post_all_public
7ye39fo49fd5dmp5dzut994deh	3/12/2020 0:33	iiqshfuenc		system_user system_user_access_token system_post_all_public
kxbyq7su9fn3zn8615kai6cj1w	4/6/2020 0:54	wi82hfh8ewu		system_user system_user_access_token system_post_all_public
dcgfe5u34jdu88cm5jt7grh44o	4/6/2020 1:10	hh88938kjshf		system_user system_user_access_token system_post_all_public
stmd1d9nqtnwu8otgp1y358c6c	7/23/2020 4:46	testtest		system_user system_user_access_token system_post_all_public
u1qd3zie5ighdpgu5dn7nato7w	7/23/2020 5:39	test1234test		system_user system_user_access_token system_post_all_public
fz1cf1odcjrzby8xuxjg1qt71h	7/24/2020 5:59	werjkl		system_user system_user_access_token system_post_all_public
4b4fbbymzpfjzfihhf6tdqb7ce	7/24/2020 6:05	tyunbv		system_user system_user_access_token system_post_all_public
ykugfn89qtbmtboru9uemkjgtc	8/12/2020 4:25	cz1299		system_user system_user_access_token system_post_all_public
a9romaora3yp8cx6s6kagxcuby	8/12/2020 4:31	oik319		system_user system_user_access_token system_post_all_public
seh4grykcjf1mqs1weqt8rnc1a	8/12/2020 4:59	ilsv34vgfk		system_user system_user_access_token system_post_all_public
irmiuq4y1jgt5f3ebsse51kbrw	9/3/2020 23:39	hsd883h99f		system_user system_user_access_token system_post_all_public
41tqbxsec7rnzf9xo6n34koney	9/17/2020 0:59	wofjeu81		system_user system_user_access_token system_post_all_public

open on a new tab

Figure 4. Mattermost server users' accounts

At the time of research, we found 15 users that are classified as follows:

User type	Count
Bot user	1
Regular user	13
Admin user	1

Table 1. Type and number of users created in the Mattermost server

We have reached out to Mattermost regarding the abuse of the platform. Here is their official statement: "Mattermost's open-source, self-managed collaboration platform is broadly used and co-created by developers and ethical security researchers. As a community, we denounce illicit and unethical use, which is explicitly against Mattermost's Conditions of Useopen on a new tab policy. We are grateful to our friends at Trend Micro for their

contributions on this issue. For more information on how to help, see: How do I report illicit use of Mattermost software?open on a new tab"

For more information and in-depth analysis of the SLUB malware's recent campaign, read our research paper, "Operation Earth Kitsune: Tracking SLUB's Current Operations"open on a new tab, which aims to shed light on SLUB's recent activities by analyzing the behavior of this quickly evolving malware.

HIDE

Like it? Add this infographic to your site:

1. Click on the box below. 2. Press Ctrl+A to select all. 3. Press Ctrl+C to copy. 4. Paste the code into your page (Ctrl+V).

Image will appear the same size as you see above.

We Recommend

-
-
-
-

- The Industrialization of Botnets: Automation and Scale as a New Threat Infrastructurenews article
- Complexity and Visibility Gaps in Power Automatenews article
- Cracking the Isolation: Novel Docker Desktop VM Escape Techniques Under WSL2news article
- Azure Control Plane Threat Detection With TrendAI Vision One™news article
- The AI-fication of Cyberthreats: Trend Micro Security Predictions for 2026predictions
- Ransomware Spotlight: DragonForcenews article
- Stay Ahead of AI Threats: Secure LLM Applications With Trend Vision Onenews article
- The Road to Agentic AI: Navigating Architecture, Threats, and Solutionsnews article

---