The Trail of BlackTech's Cyber Espionage Campaigns

By By: Lenart Bermejo, Razor Huang, CH Lei Jun 22, 2017 Read time: 6 min (1639 words)

Published: 2017-06-22 · Archived: 2026-04-02 11:15:29 UTC

BlackTech is a cyber espionage group operating against targets in East Asia, particularly Taiwan, and occasionally, Japan and Hong Kong. Based on the mutexes and domain names of some of their C&C servers, BlackTech's campaigns are likely designed to steal their target's technology.

Following their activities and evolving tactics and techniques helped us uncover the proverbial red string of fate that connected three seemingly disparate campaigns: PLEAD, Shrouded Crossbow, and of late, Waterbear.

Over the course of their campaigns, we analyzed their modus operandi and dissected their tools of the trade—and uncovered common denominators indicating that PLEAD, Shrouded Crossbow, and Waterbear may actually be operated by the same group.

PLEAD

PLEAD is an information theft campaign with a penchant for confidential documents. Active since 2012, it has so far targeted Taiwanese government agencies and private organizations. PLEAD's toolset includes the self-named PLEAD backdoor and the DRIGO exfiltration tool. PLEAD uses spear-phishing emails to deliver and install their backdoor, either as an attachment or through links to cloud storage services. Some of the cloud storage accounts used to deliver PLEAD are also used as drop off points for exfiltrated documents stolen by DRIGO.

PLEAD's installers are disguised as documents using the right-to-left-overrideopen on a new tab (RTLO) technique to obfuscate the malware's filename. They are mostly accompanied by decoy documents to further trick users. We've also seen PLEAD use exploits for these vulnerabilities:

- CVE-2015-5119, patched by Adobe last July, 2015
- CVE-2012-0158, patchedopen on a new tab by Microsoft last April, 2012
- CVE-2014-6352, patchedopen on a new tab by Microsoft last October, 2014
- CVE-2017-0199, patchedopen on a new tab by Microsoft last April, 2017

PLEAD also dabbled with a short-lived, fileless version of their malware when it obtained an exploit for a Flash vulnerability (CVE-2015-5119) that was leaked during the Hacking Team breachnews article.

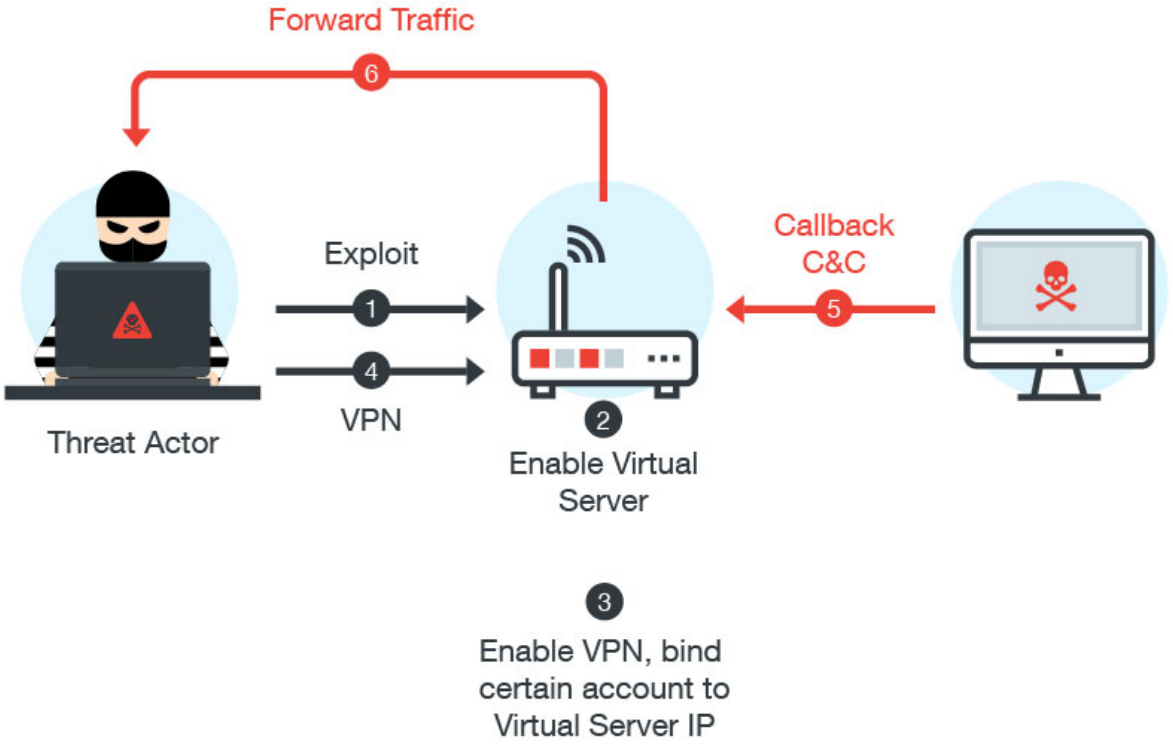

Figure 1: How PLEAD utilizes compromised routers

PLEAD actors use a router scanner tool to scan for vulnerable routers, after which the attackers will enable the router's VPN feature then register a machine as virtual server. This virtual server will be used either as a C&C server or an HTTP server that delivers PLEAD malware to their targets.

PLEAD also uses CVE-2017-7269, a buffer overflow vulnerability Microsoft Internet Information Services (IIS) 6.0open on a new tab to compromise the victim's server. This is another way for them to establish a new C&C or HTTP server.

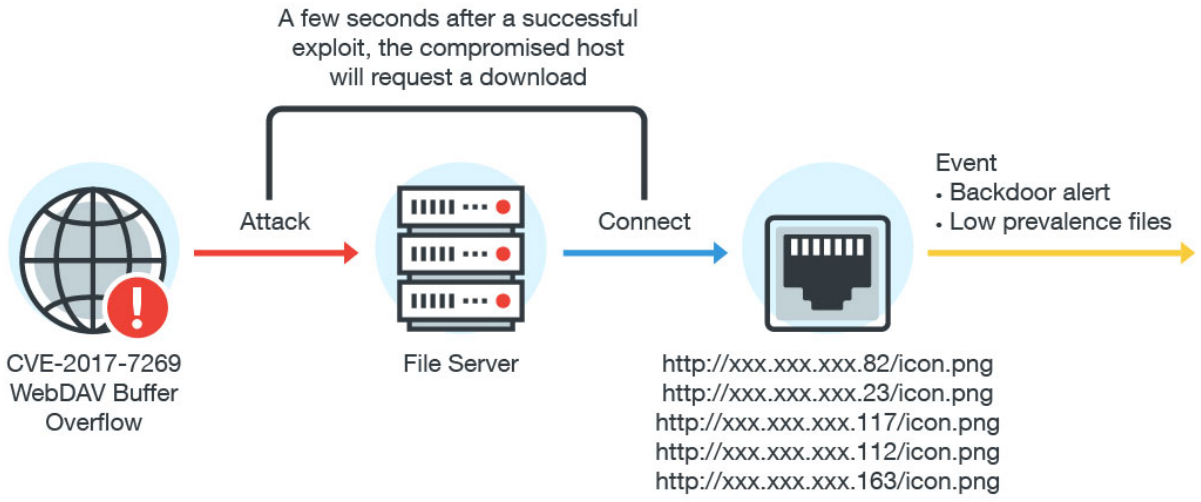

Figure 2: One of the methods PLEAD operators use to distribute their malware

PLEAD's backdoor can:

- Harvest saved credentials from browsers and email clients like Outlook
- List drives, processes, open windows, and files
- Open remote Shell
- Upload target file
- Execute applications via *ShellExecute* API
- Delete target file

PLEAD also uses the document-targeting exfiltration tool DRIGO, which mainly searches the infected machine for documents. Each copy of DRIGO contains a refresh token tied to specific Gmail accounts used by the attackers, which are in turn linked to a Google Drive account. The stolen files are uploaded to these Google Drives, where the attackers can harvest them.

Shrouded Crossbow

This campaign, first observed in 2010, is believed to be operated by a well-funded group given how it appeared to have purchased the source code of the BIFROST backdoor, which the operators enhanced and created other tools from. Shrouded Crossbow targeted privatized agencies and government contractors as well as enterprises in the consumer electronics, computer, healthcare, and financial industries.

Shrouded Crossbow employs three BIFROST-derived backdoors: BIFROSE, KIVARS, and XBOW. Like PLEAD, Shrouded Crossbow uses spear-phishing emails with backdoor-laden attachments that utilize the RTLO technique and accompanied by decoy documents.

BIFROSE, known for evading detection by communicating with its C&C servers via Tor protocol, also has a version targeting UNIX-based operating systems, which are usually used in servers, workstations, and mobile devices. KIVARS has less functionality than BIFROSE, but its modular structure made it easier to maintain. KIVARS enabled attackers to download and execute files, list drives, uninstall malware service, take screenshots, activate/deactivate keylogger, show/hide active windows, and trigger mouse clicks and keyboard inputs. A 64-bit version of KIVARS also emerged to keep pace with the popularity of 64-bit systems. XBOW's capabilities are derived from BIFROSE and KIVARS; Shrouded Crossbow gets its name from its unique mutex format.

Waterbear

Waterbear has actually been operating for a long time. The campaign's name is based on its malware's capability to equip additional functions remotely.

Waterbear similarly employs a modular approach to its malware. A loader component executable will connect to the C&C server to download the main backdoor and load it in memory. A later version of this malware appeared and used patched server applications as its loader component, while the main backdoor is either loaded from an encrypted file or downloaded from the C&C server.

The tactic it later adopted required prior knowledge of their targets' environment. It's possible attackers used Waterbear as a secondary payload to help maintain presence after gaining some levels of access into the targets' systems.

All Roads Lead to BlackTech

Based on the use of the same C&C servers, the campaigns' coordinated efforts, and similarities in tools, techniques, and objectives, we can conclude that they are operated by the same group. It is not uncommon, for instance, for a group—especially a well-funded one—to split into teams and run multiple campaigns. While most of the campaigns' attacks are conducted separately, we've seen apparently joint operations conducted in phases that entail the work of different teams at each point in the infection chain.

Use of the Same C&C Servers. In several instances, we found the campaigns' malware communicating with the same C&C servers. In targeted attacks, C&C servers are typically not shared with other groups. Here are some of the C&C servers we found that are shared by the campaigns:

C&C Server	PLEAD	Shrouded Crossbow	Waterbear
itaiwans[.]com	Yes	No	Yes
microsoftmse[.]com	Yes	Yes	No
211[.]72[.]242[.]120	Yes	Yes	No

Table 1: C&C servers shared by PLEAD, Shrouded Crossbow, and Waterbear

Additionally, the IP 211[.]72 [.]242[.]120 is one of the hosts for the domain microsoftmse[.]com, which has been used by several KIVARS variants.

Joint Operations. We also found incidents where the backdoors were used on the same targets. While it's possible for separate groups to attack at the same time, we can construe at they are at least working together:

	PLEAD	Shrouded Crossbow
Samples from different groups using the same filename	Loader component named after its target, i.e. *{target name}.exe*	Loader component named after its target, i.e. *{target name}.exe* or *{target name}64.exe*
Backdoors using the same C&C servers	Connected to 211[.]72[.]242[.]120:53	Connected to 211[.]72[.]242[.]120:443
Timeline indicating arrival order	Arrived two days after initial infection by SC	Established presence two years prior, but re-infected at a recent time

Table 2: Incident where PLEAD and KIVARS attack the same target

	PLEAD	Shrouded Crossbow	Waterbear

Samples found in same machine	*vmdks.exe*	*cfbcjtqx.dll*	*tpauto.dll*
Timeline of infection	3/16/2017	2/23/2017	3/8/2017

Table 3: Incidents where PLEAD, KIVARS, and Waterbear were used on the same target

Similarities between tools and techniques. PLEAD and KIVARS, for instance, share the use of RTLO techniques to disguise their installers as documents. Both also use decoy documents to make the RTLO attack more convincing. Another similarity is the use of a small loader component to load encrypted backdoors into memory.

Similar Objectives. The ulterior motive of these campaigns is to steal important documents from their victims; initial recipients of their attacks are not always their primary target. For instance, we saw several decoy documents stolen by the attackers that are then used against another target. This indicates that document theft is most likely the first phase of an attack chain against a victim with ties to the intended target. While PLEAD and KIVARS are most likely to be used in first phase attacks, Waterbear can be seen as a secondary backdoor installed after attackers have gained a certain level of privilege.

Based on the type of documents stolen by these campaigns, we can get a clearer view of who they're targeting and compromising, the purpose of their campaigns, and when they take place. Below are some of the categories or labels of the stolen documents:

- Address book
- Budget
- Business
- Contract
- Culture
- Defense
- Education
- Energy
- Foreign affairs
- Funding application
- Human affairs
- Internal affairs
- Laws
- Livelihood economy
- Meeting
- Official letter
- Password list
- Performance appraisal
- Physical culture
- Press release
- Public security
- Schedule

Enterprises Need to be Proactive

PLEAD, Shrouded Crossbow, and Waterbear are still actively mounting their campaigns against its targets, which is why organizations must proactively secure their perimeter.

IT/system administrators and information security professionals can consider making a checklist of what to look out for in the network for any signs of anomalies and suspicious behavior that can indicate intrusions. Adopting best practicesnews article and employing multilayered security mechanisms and strategies against targeted attacks are also recommended. Network traffic analysisnews article, deployment of firewallsnews article and intrusion detection and prevention systems, network segmentation, and data categorization are just some of them.

Trend Micro Solutions

Trend Micro™ Deep Discovery™ provides detection, in-depth analysis, and proactive response to today's stealthy malware, and targeted attacks in real-time. It provides a comprehensive defense tailored to protect organizations against targeted attacks and advanced threats through specialized engines, custom sandboxing, and seamless correlation across the entire attack lifecycle, allowing it to detect threats like the above mentioned zero-day attacks even without any engine or pattern update.

Trend Micro™ Deep Security™ and Vulnerability Protection provide virtual patching that protects endpoints from threats that abuses unpatched vulnerabilities. OfficeScan's Vulnerability Protection shield endpoints from identified and unknown vulnerability exploits even before patches are deployed.

Trend Micro™ Smart Protection with Maximum XGen™ security infuses high-fidelity machine learning into a blend of threat protection techniques to eliminate security gaps across user activity and any endpoint—the broadest possible protection against advanced attacks. An overview and analysis of the various malware used by PLEAD, Shrouded Crossbow, and Waterbear, along with their Indicators of Compromise (hashes, C&Cs), can be found in this **technical brief**.
