IMAGE: DAVID B. GLEASON

Martin Matishak | January 11, 2022

How the Pentagon enlisted ethical hackers amid the Log4j crisis

Government Malware News

The Pentagon last month pivoted an ongoing bug bounty program to track down Log4j vulnerabilities on potentially thousands of public-facing military websites, the first time the Defense Department marshaled the ethical hacker community to tackle an emerging digital crisis.

The Defense Digital Service broadened the scope of a competition that was underway to test its own systems and software, run in collaboration with bug bounty platform HackerOne, just days after the public became aware of the security flaw during the second week of December in a bid to help the broader department address the unfolding threat.

“It was a really quick effort, and a really elegant solution, to use a contract that we already had in place with the crowdsource research community to very quickly do a scan of what might be affected within the DoD,” acting DDS Director Katie Olson told *The Record* during an interview last week.

Within days, the roughly 50 vetted cybersecurity researchers participating in the hunt — the latest in a series that began with 2016’s “Hack the Pentagon” initiative that led the department to expand its Vulnerability Disclosure Program last year to include all publicly accessible DoD information systems — were given an additional assignment: scour all .mil websites and report any potential weaknesses or exploits caused by the widely-used internet software.

The on-the-fly change coincided with a decision by the Homeland Security Department — which had just launched its inaugural bug bounty program and whose Cybersecurity and Infrastructure Security Agency (CISA) has become home to a few DDS alums — to broaden the nascent effort to incorporate Log4j vulnerabilities as well.

Major tech companies and federal officials have scrambled to grasp the full extent of the Log4j flaw, warning that potentially hundreds of millions of devices around the globe could be compromised. CISA last month issued an emergency directive requiring all civilian federal agencies to mitigate the threat, though top agency officials on Monday repeated that they have not seen a malicious actor use the vulnerability to breach federal departments and agencies.

On a call with reporters, Eric Goldstein, CISA’s executive assistant director for cybersecurity, noted that researchers had helped uncover 17 previously unidentified assets that were vulnerable to Log4j, “all which were remediated before any intrusion could occur.”

“It demonstrated the extraordinary power of crowdsourcing the research community to help not only the U.S. government but the broader nation find vulnerabilities before the adversary can use them,” he said.

A BUG BOUNTY EVENT FOR THE US AIR FORCE HELD IN NEW YORK CITY IN 2017. IMAGE: HACKERONE

The Pentagon uses an ecosystem of passive scanning software and technology to continuously monitor its assets. But Log4j differs from previous cyber incidents in that it doesn't center around specific kinds of hardware or software, such as virtual private network endpoints in firewall devices.

Distributed for free by the nonprofit Apache Software Foundation and downloaded millions of times, Log4j is one of the most ubiquitous digital tools in the world. Anything written in Java programming language can be affected by the bug — from a web server to an application. While an automated system might successfully ferret out questionable code, it can't judge if it can ultimately be exploited by hackers.

"That's the quandary we found. There's no real good, automated solution to hunt down and figure out, 'Hey, this is vulnerable, and it's exploitable,'" Lance Cleghorn, a digital services expert at DDS, told *The Record*. "That's where the crowd really comes in to save the day. They can not only tell you, 'Hey, I actually went and found this is vulnerable — definitely. Here's the evidence.' But also: 'It's exploitable, and that's a problem.'"

At first blush, public-facing military websites may not seem like an attractive target for hackers. However, there has long been concern within DoD that a sophisticated threat actor could use a previously unknown vulnerability to penetrate its networks and gain a foothold in the department's systems, like the massive Nonclassified Internet Protocol Router Network (NIPRnet).

In a statement, HackerOne CISO and Chief Hacking Officer Chris Evans said that once the bug bounty was expanded to include Log4j hackers "responded immediately and competently, with numerous valid reports pouring in within the first few hours."

DDS has paid competitors $500 for each uncovered vulnerability and an additional $500 if it's proven the weakness can be exploited. Each reported discovery is referred to DoD's Cyber Crime Center, which runs the department's VDP effort, and then shares it with the Joint Force Headquarters-Department of Defense Information Network (JFHQ-DODIN) for remediation.

Both Olson and Cleghorn declined to say how many vulnerabilities have been found during the retooled bug bounty, which is slated to wrap up on Friday.

"We've paid out a chunk already," Cleghorn said, later suggesting there could be some kind of follow-on effort to the hunt.

"This might still be of interest to the greater DoD community."

Olson said she hopes the effort spurs more government agencies to establish their own bug bounty programs, stressing that technical talent and contracting mechanisms must be in place before an organization could potentially call on white hat researchers to help with emergency incidents.

"The vulnerability was found and three days later we were able to launch this program. If you know anything about federal contracting, that's sort of unheard of," she joked.

"This is becoming a new reality," Olson added. "So having something like this in place, and being able to tap in quickly to our research community and a contracting vehicle, having an infrastructure in place is going to be more and more important."

Tags

bug bounty Department of Defense HackerOne malware Pentagon vulnerability

Martin is a cybersecurity reporter for The Record. He spent the last five years at Politico, where he covered Congress, the Pentagon and the U.S. intelligence community and was a driving force behind the publication's cybersecurity newsletter.

‹ Previous article Next article ›

BRIEFS

EA blames support staff for recent hacks of high-profile FIFA accounts | January 11, 2022

US warns of Russian state-sponsored attacks on critical infrastructure | January 11, 2022

SFile (Escal) ransomware ported for Linux attacks | January 10, 2022

CISA director: Log4Shell has not resulted in 'significant' government intrusions yet | January 10, 2022

Ransomware tracker: the latest figures [January 2022] | January 10, 2022

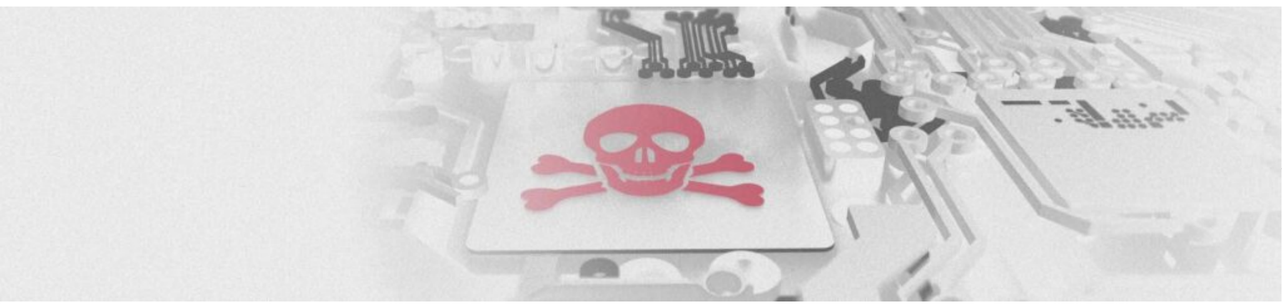
Salesforce to require MFA for all users starting next month | January 7, 2022

Booking management platform FlexBooker leaks 3.7 million user records | January 6, 2022

Google Docs commenting feature abused in phishing operations | January 6, 2022

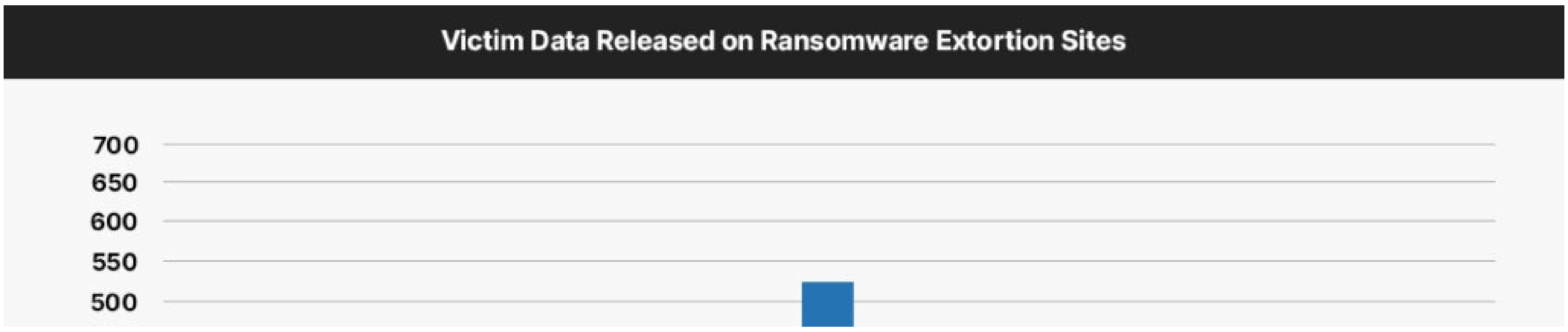
INSIKT GROUP® RESEARCH

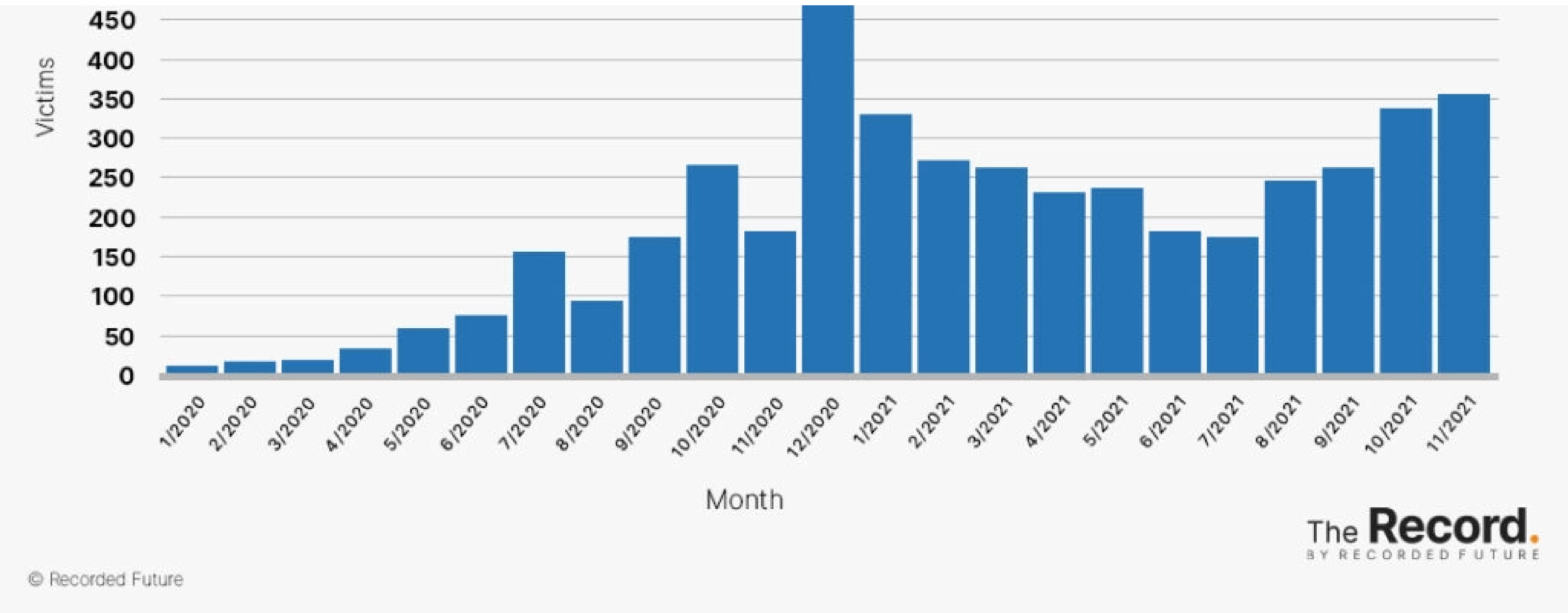
Log4Shell: How It's Being Exploited and How to Mitigate Damage | 2021-12-14 14:55:00



A vulnerability in Log4j can execute remote code with the full privileges of the main program. The exploit has been dubbed Log4Shell.

RANSOMWARE TRACKER: THE LATEST FIGURES [JANUARY 2022]





RANSOMWARE TRACKER: THE LATEST FIGURES [JANUARY 2022]

The Record.
BY RECORDED FUTURE

About Us Privacy Policy