Hackers target Ukrainian govt with IcedID malware, Zimbra exploits

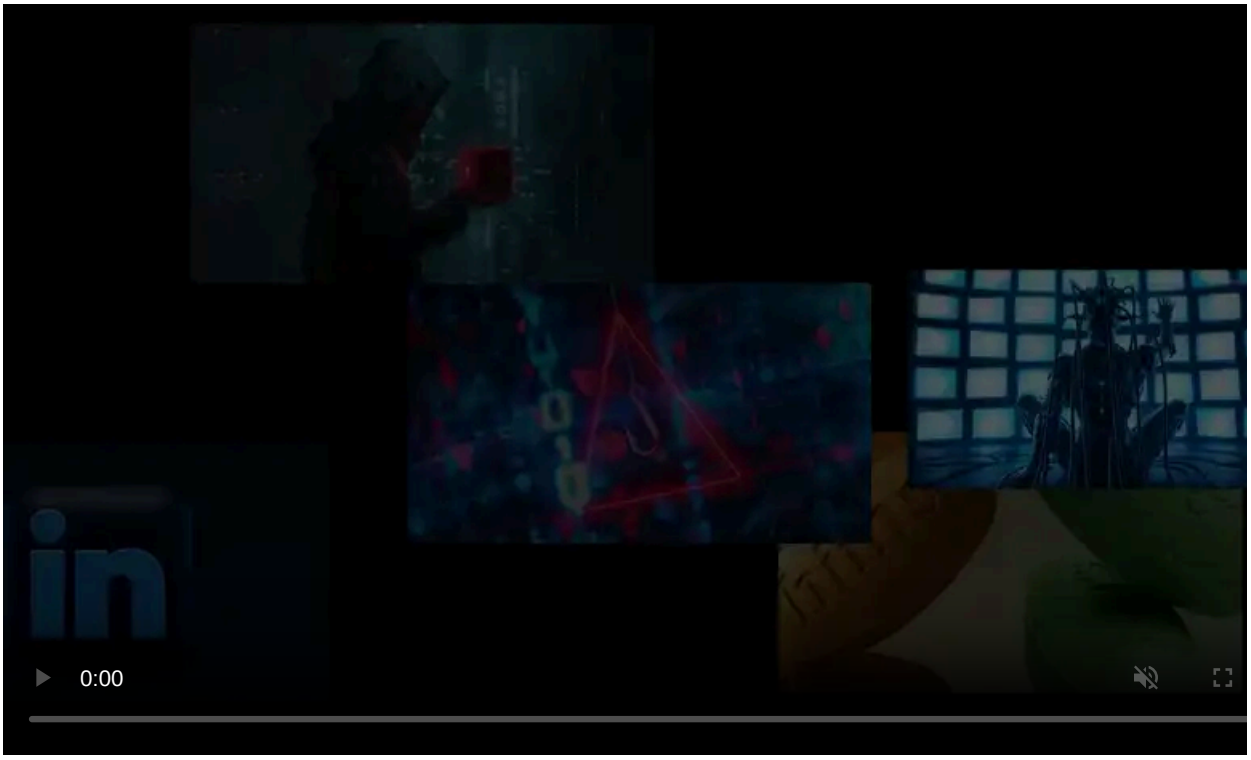
By Bill Toulas

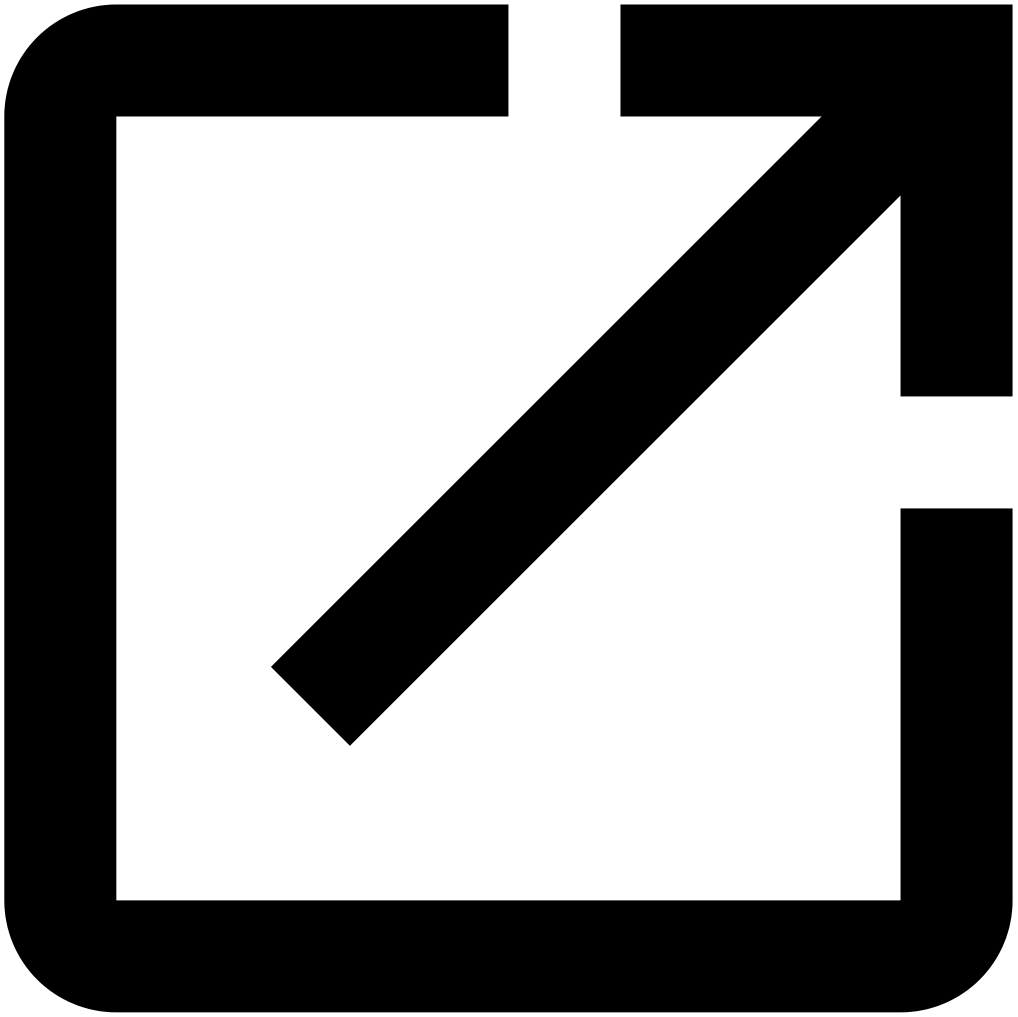
Published: 2022-04-14 · Archived: 2026-04-05 17:47:22 UTC

Hackers are targeting Ukrainian government agencies with new attacks exploiting Zimbra exploits and phishing attacks pushing the IcedID malware.

The Computer Emergency Response Team of Ukraine (CERT-UA) detected the new campaigns and attributed the IcedID phishing attack to the UAC-0041 threat cluster, previously connected with AgentTesla distribution, and the second to UAC-0097, a currently unknown actor.

Although attributions are moderately confident, this is another snapshot of the malicious cyber-activity targeting Ukrainian entities.


0:00



Visit Advertiser websiteGO TO PAGE

In both cases, the goal of the threat actors is to gain access to internal networks to perform cyber-espionage on Ukraine's most critical government agencies.

IcedID infecting state orgs

The first report describes a campaign distributing XLS documents named "Mobilization Register.xls," reaching many recipients.

Opening the document requests the user to "Enable the Content" for viewing, resulting in a malicious macro executing to download and run a malicious file.

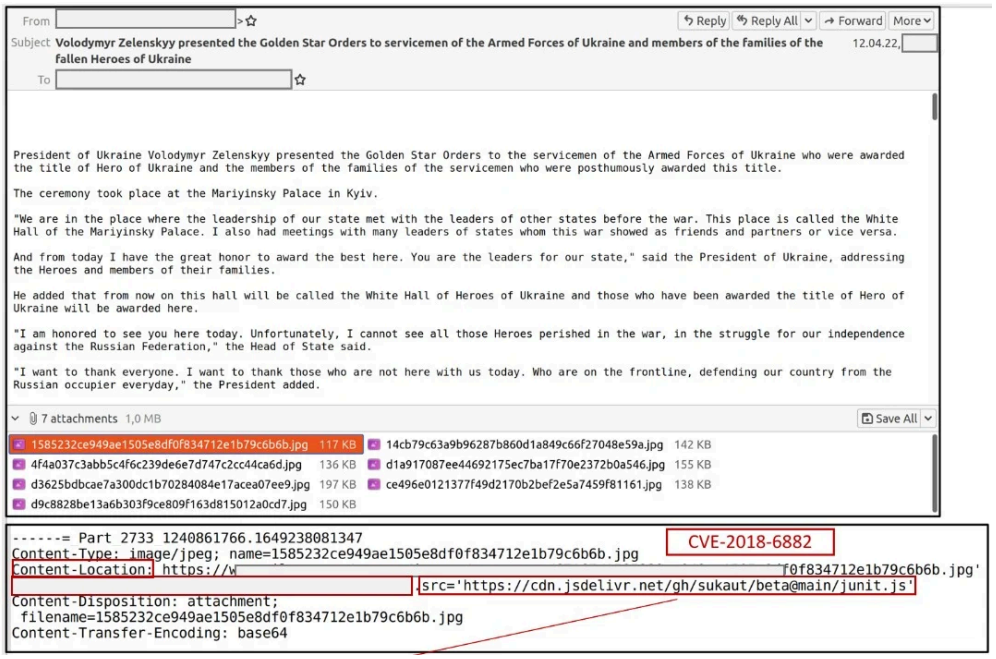
This file is the GzipLoader malware, which fetches, decrypts, and executes the final payload, IcedID (aka BankBot).

IcedID is a modular banking trojan that can be used for stealing account credentials or as a loader of additional, second-stage malware such as Cobalt Strike, ransomware, wipers, and more.

Details from the IcedID campaign *(CERT-UA)*

Spying on government emails

The second report involves an email sent to government agencies in Ukraine, with attached images allegedly from an event where President V. Zelensky awarded Armed Forces members.



Email with malicious jpg attachments *(CERT-UA)*

The attached images contain a content-location header that links to a web resource hosting JavaScript code that triggers the exploitation of the Zimbra CVE-2018-6882 vulnerability.

This cross-site scripting vulnerability affects Zimbra Collaboration Suite versions 8.7 and older, enabling remote attackers to inject arbitrary web script or HTML via a content-location header in email attachments.

Zimbra is an email and collaboration platform that also includes instant messaging, contacts, video conferencing, file sharing, and cloud storage capabilities.

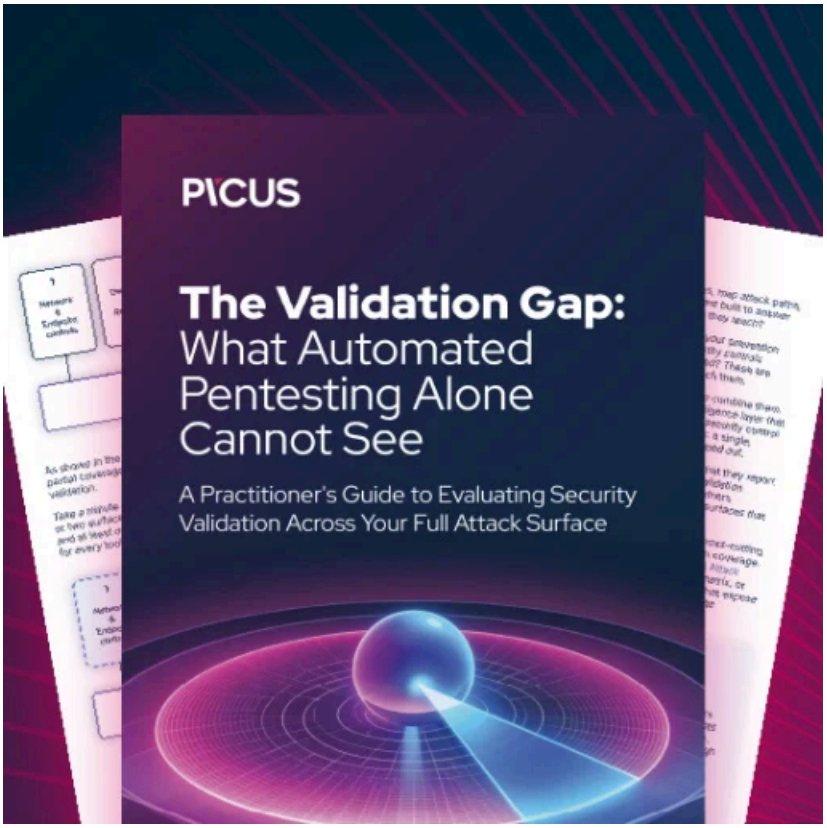
In this case, exploiting the flaw adds a forwarding rule for the victim's emails to a new address under the threat actor's control, which is clearly an espionage-supporting move.

Setting Zimbra to forward victim's emails *(CERT-UA)*

It is worth noting that Zimbra had a similar XSS problem earlier this year, affecting the most recent 8.8.15 P29 & P30 versions of the suite.

That flaw was actively exploited as a zero-day by Chinese threat actors who used it to steal the emails of European media and government organizations.

As such, CERT-UA advises all organizations in Ukraine using Zimbra to update to the latest available versions of the suite immediately.



Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: https://www.bleepingcomputer.com/news/security/hackers-target-ukrainian-govt-with-icedid-malware-zimbra-exploits/