URSNIF, EMOTET, DRIDEX and BitPaymer Gangs Linked by a Similar Loader

- Posted on:December 18, 2018 at 4:51 am
- Posted in:Botnets, Malware
- Author:
  Trend Micro

0

As ransomware and banking trojans captured the interest – and profits – of the world with their destructive routines, cybersecurity practitioners have repeatedly published online and offline how cybercriminals have compartmentalized their schemes through exchange of information and banded professional organizations. As a more concrete proof of the way these symbiotic relationships and work flows intersect, we discovered a connection between EMOTET, URSNIF, DRIDEX and BitPaymer from open source information and the loaders of the samples we had, functioning as if tasks were divided among different developers and operators.

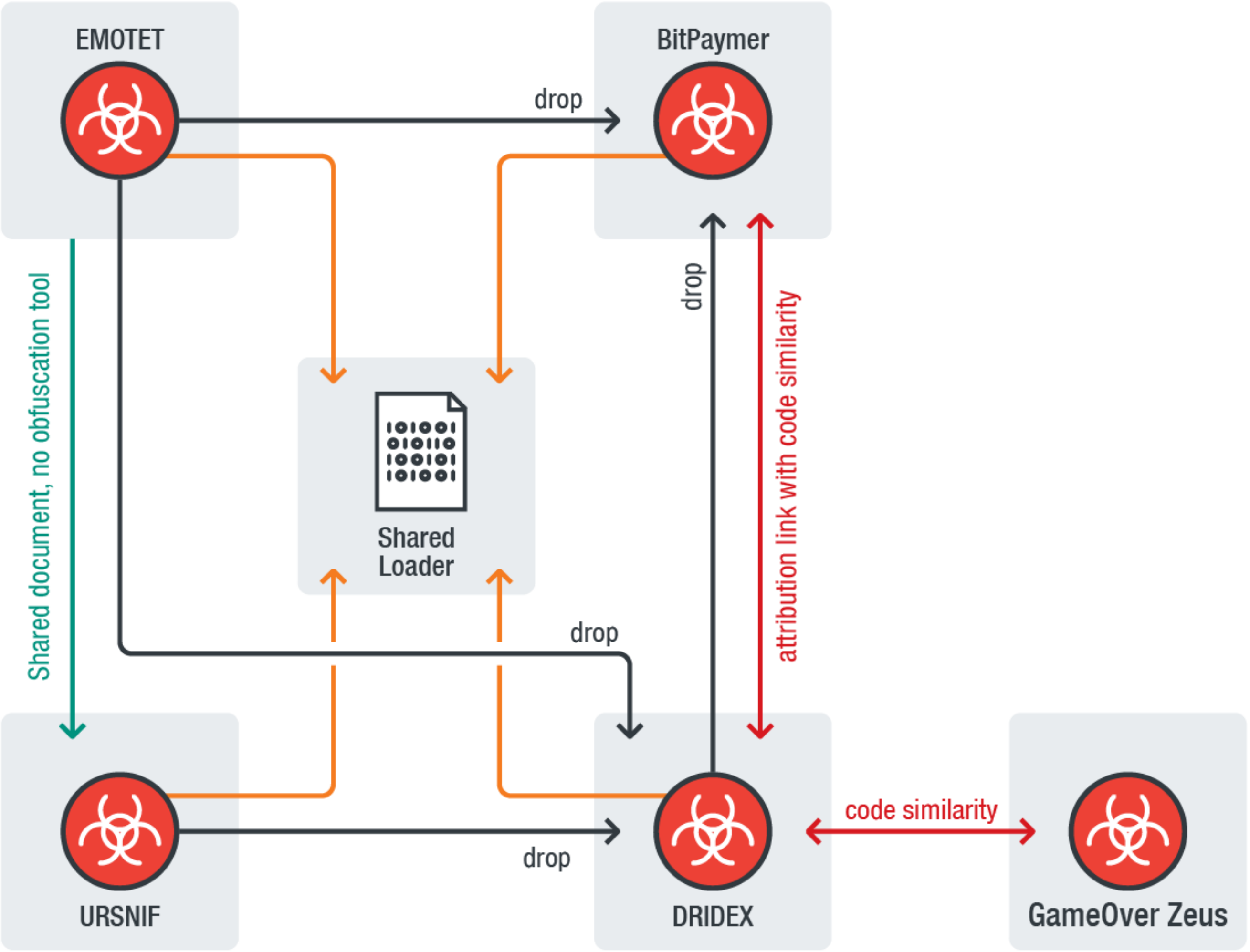


Figure 1. Connections of EMOTET, DRIDEX, URSNIF and BitPaymer.

Background and details

In order to have a better understanding of the significance of these connections, here's a summarized background of each malware family:

- URSNIF / GOZI-ISFB

Still considered as one of the global top threats, this banking trojan's source code was among those repeatedly leaked because of its evolution and notoriety for adaptive behaviors. This spyware monitors traffic, features a keylogger, and steals credentials stored in browsers and applications. The malware creators of GOZI admitted to its creation and distribution, and was sentenced in 2015 and 2016.

- DRIDEX

Another banking trojan that targets banking and financial institutions, the cybercriminals behind it use various methods and techniques to steal personal information and credentials through malicious attachments and HTML injections. DRIDEX evolved from CRIDEX, GameOver Zeus and ZBOT, and proved to be resilient even after it was momentarily taken down in 2015 through a partnership with the FBI.

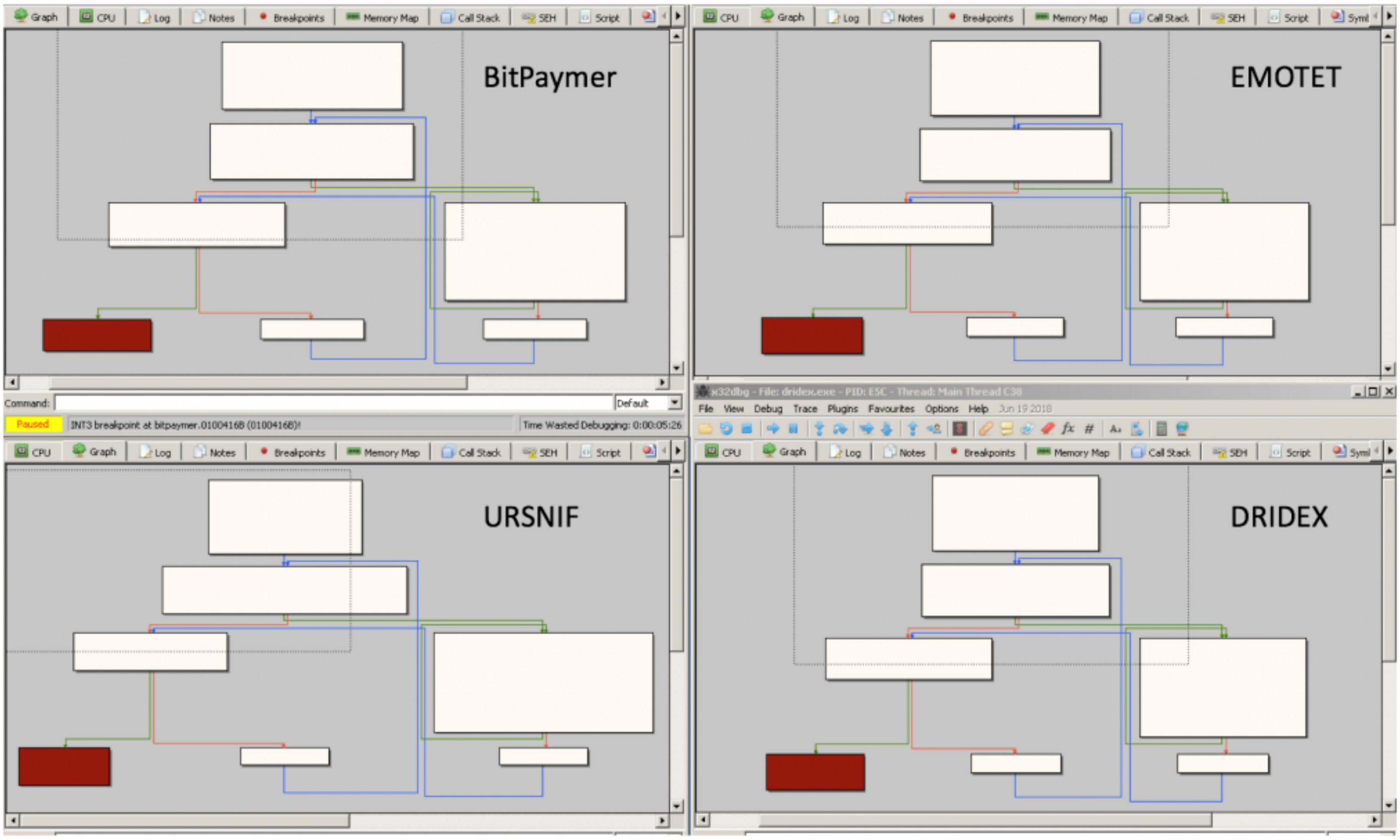
- EMOTET

Discovered by Trend Micro in 2014, this malware acts as a loader for payloads such as Gootkit, ZeusPanda, IcedID, TrickBot, and DRIDEX for critical attacks. Other publications have also mentioned observing obfuscation techniques between EMOTET and URSNIF/GOZI-ISFB.

- BitPaymer

This ransomware was used to target medical institutions via remote desktop protocol and other email-related techniques, momentarily shutting down routine services for a high ransom. Security researchers later published evidence that not only was DRIDEX dropping BitPaymer, but that it also came from the same cybercriminal group.

During our analysis, we found evidence that the malware families identified had shared loaders: the overview of the payload decryption procedure, and the loaders' internal data structure. While the first figure of the disassembled PE packers had small differences in their arithmetic operations' instructions, we found that the four payload decryption procedures were identical in data structures' overview on the way they decrypted the actual PE payloads.



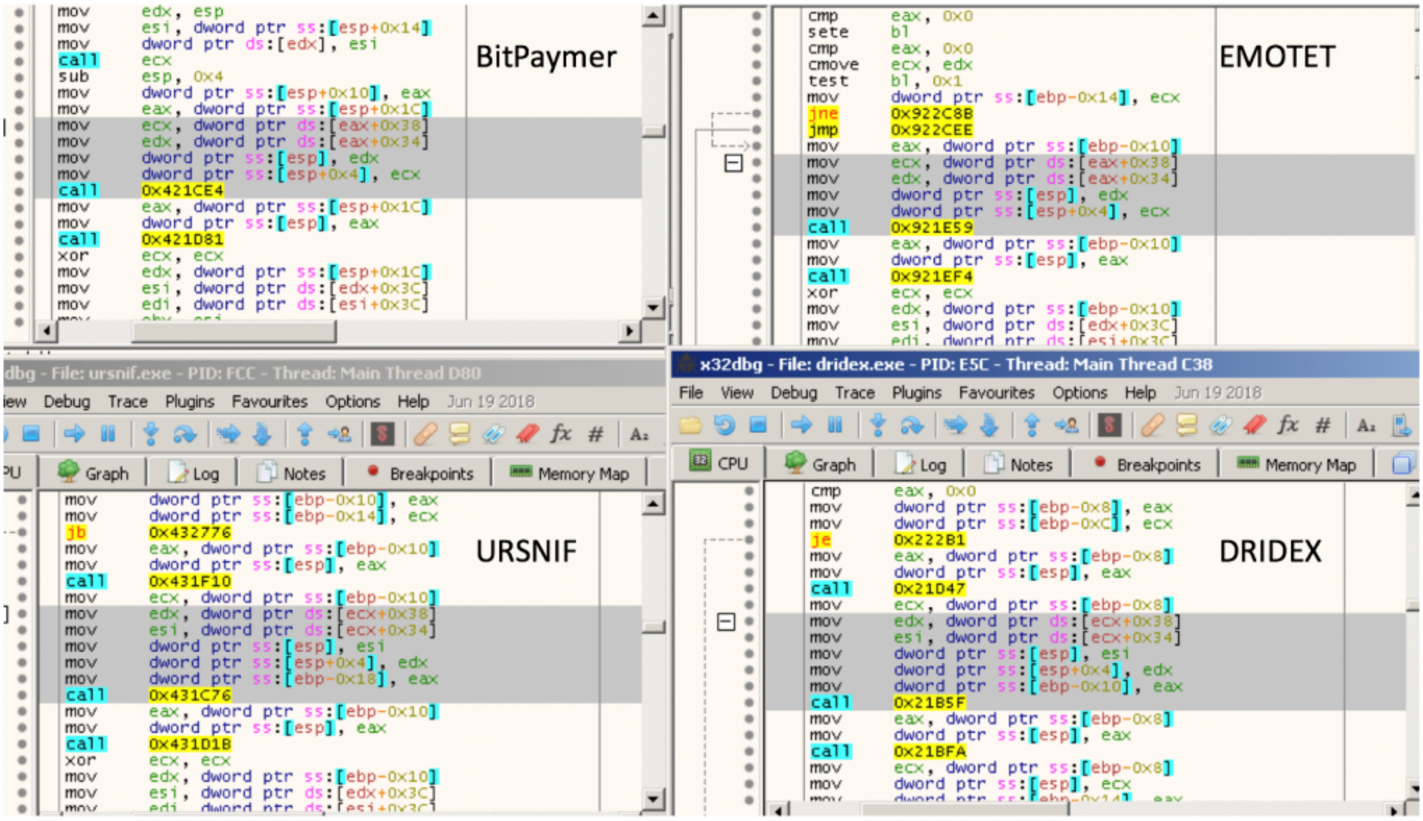
INT3 breakpoint at bitpaymer.01004168 (01004168)!

Time Wasted Debugging: 0:00:05:26

x32dbg - File: dridex.exe - PID: E5C - Thread: Main Thread C38

Figure 2. Overview of identical structures of payloads' loader decryption procedures.

Further analysis also revealed that the internal data structure of the four malware families were the same. We compared the disassembled codes from the samples we had and noticed the encrypted payload address and size placed into the decryption procedure located at offset 0x34 and 0x38.


BitPaymer
EMOTET
URSNIF
DRIDEX
File View Debug Trace Plugins Favourites Options Help Jun 19 2018
CPU
Graph
Log
Notes
Breakpoints
Memory Map

```
mov     edx, esp
mov     esi, dword ptr ss:[esp+0x14]
mov     dword ptr ds:[edx], esi
call    ecx
sub     esp, 0x4
mov     dword ptr ss:[esp+0x10], eax
mov     eax, dword ptr ss:[esp+0x1C]
mov     ecx, dword ptr ds:[eax+0x38]
mov     edx, dword ptr ds:[eax+0x34]
mov     dword ptr ss:[esp], edx
mov     dword ptr ss:[esp+0x4], ecx
call    0x421CE4
mov     eax, dword ptr ss:[esp+0x1C]
mov     dword ptr ss:[esp], eax
call    0x421D81
xor     ecx, ecx
mov     edx, dword ptr ss:[esp+0x1C]
mov     esi, dword ptr ds:[edx+0x3C]
mov     edi, dword ptr ds:[esi+0x3C]
```

```
cmp     eax, 0x0
sete    bl
cmp     eax, 0x0
cmove   ecx, edx
test    bl, 0x1
mov     dword ptr ss:[ebp-0x14], ecx
jne     0x922C8B
jmp     0x922CEE
mov     eax, dword ptr ss:[ebp-0x10]
mov     ecx, dword ptr ds:[eax+0x38]
mov     edx, dword ptr ds:[eax+0x34]
mov     dword ptr ss:[esp], edx
mov     dword ptr ss:[esp+0x4], ecx
call    0x921E59
mov     eax, dword ptr ss:[ebp-0x10]
mov     dword ptr ss:[esp], eax
call    0x921EF4
xor     ecx, ecx
mov     edx, dword ptr ss:[ebp-0x10]
mov     esi, dword ptr ds:[edx+0x3C]
```

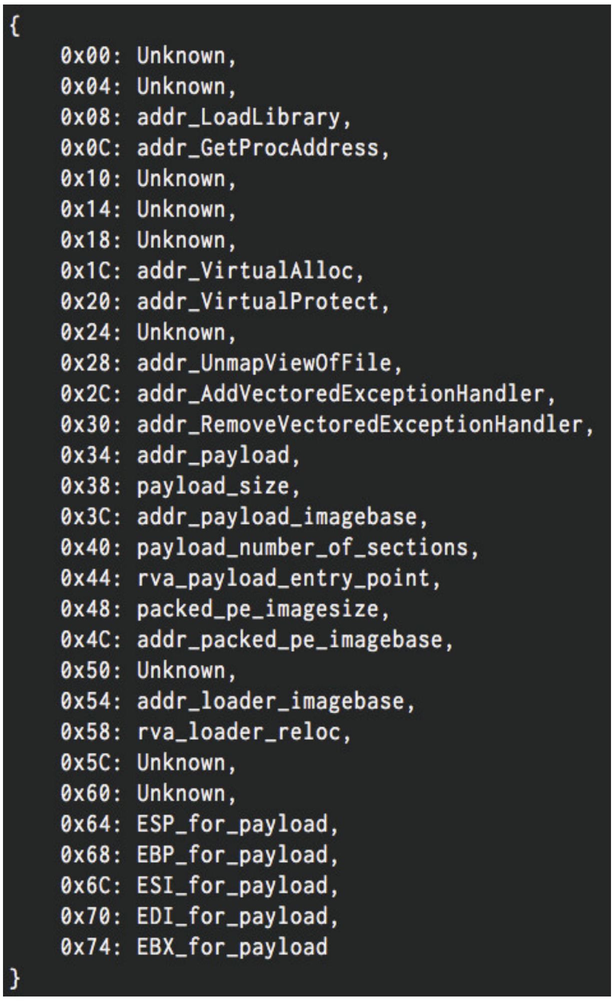
dbg - File: ursnif.exe - PID: FCC - Thread: Main Thread D80

```
mov     dword ptr ss:[ebp-0x10], eax
mov     dword ptr ss:[ebp-0x14], ecx
jb      0x432776
mov     eax, dword ptr ss:[ebp-0x10]
mov     dword ptr ss:[esp], eax
call    0x431F10
mov     ecx, dword ptr ss:[ebp-0x10]
mov     edx, dword ptr ds:[ecx+0x38]
mov     esi, dword ptr ds:[ecx+0x34]
mov     dword ptr ss:[esp], esi
mov     dword ptr ss:[esp+0x4], edx
mov     dword ptr ss:[ebp-0x18], eax
call    0x431C76
mov     eax, dword ptr ss:[ebp-0x10]
mov     dword ptr ss:[esp], eax
call    0x431D1B
xor     ecx, ecx
mov     edx, dword ptr ss:[ebp-0x10]
mov     esi, dword ptr ds:[edx+0x3C]
```

x32dbg - File: dridex.exe - PID: E5C - Thread: Main Thread C38

```
cmp     eax, 0x0
mov     dword ptr ss:[ebp-0x8], eax
mov     dword ptr ss:[ebp-0xC], ecx
je      0x222B1
mov     eax, dword ptr ss:[ebp-0x8]
mov     dword ptr ss:[esp], eax
call    0x21D47
mov     ecx, dword ptr ss:[ebp-0x8]
mov     edx, dword ptr ds:[ecx+0x38]
mov     esi, dword ptr ds:[ecx+0x34]
mov     dword ptr ss:[esp], esi
mov     dword ptr ss:[esp+0x4], edx
mov     dword ptr ss:[ebp-0x10], eax
call    0x21B5F
mov     eax, dword ptr ss:[ebp-0x8]
mov     dword ptr ss:[esp], eax
call    0x21BFA
mov     ecx, dword ptr ss:[ebp-0x8]
mov     dword ptr ss:[esp], ecx
```

Figure 3. Identical data structures show similar payload addresses and sizes.



```
{
    0x00: Unknown,
    0x04: Unknown,
    0x08: addr_LoadLibrary,
    0x0C: addr_GetProcAddress,
    0x10: Unknown,
    0x14: Unknown,
    0x18: Unknown,
    0x1C: addr_VirtualAlloc,
    0x20: addr_VirtualProtect,
    0x24: Unknown,
    0x28: addr_UnmapViewOfFile,
    0x2C: addr_AddVectoredExceptionHandler,
    0x30: addr_RemoveVectoredExceptionHandler,
    0x34: addr_payload,
    0x38: payload_size,
    0x3C: addr_payload_imagebase,
    0x40: payload_number_of_sections,
    0x44: rva_payload_entry_point,
    0x48: packed_pe_imagesize,
    0x4C: addr_packed_pe_imagebase,
    0x50: Unknown,
    0x54: addr_loader_imagebase,
    0x58: rva_loader_reloc,
    0x5C: Unknown,
    0x60: Unknown,
    0x64: ESP_for_payload,
    0x68: EBP_for_payload,
    0x6C: ESI_for_payload,
    0x70: EDI_for_payload,
    0x74: EBX_for_payload
}
```

Figure 4. Data structure used by the shared loader.

As cybercrime organizational structures in some countries tend to compartmentalize work, we suspect that the four malware families' gangs might be in contact with the same weapon providers for PE loaders. In addition, it's also possible that these four cybercrime groups may establish some attributional – working or otherwise – relationships and have exchanged or continue to exchange resources.

In our history of monitoring botnets and the underground organizations who make and/or use them, the cybercriminals behind EMOTET may be sharing to collaborate with trusted, highly-skilled cybercriminal groups, and may be a sign of these four groups' ongoing and intriguing relationship.

Alliances like these could lead to more destructive malware deployments in the future. More than ever, it is important for organizations to heighten cybersecurity preventive measures, such as establishing policies and procedures for handling security threats. Regular education awareness sessions and reminders for employees can help protect the enterprise from attacks and intrusions from malicious emails and URLs. Installing and updating a multi-layered protection and solution in preventing online banking threats can go a long way in securing businesses.

Trend Micro Solutions

Trend Micro endpoint solutions such as the Smart Protection Suites and Worry-Free Business Security solutions can protect users and businesses from threats by detecting malicious files and messages as well as blocking all related malicious URLs. Trend Micro™ Deep Discovery™ has an email inspection layer that can protect enterprises by detecting malicious attachments and URLs.

Trend Micro XGen™ security provides a cross-generational blend of threat defense techniques to protect systems from all types of threats, including ransomware and cryptocurrency-mining malware. It features high-fidelity machine learning on gateways and endpoints, and protects physical, virtual, and cloud workloads. With capabilities like web/URL filtering, behavioral analysis, and custom sandboxing, XGen security can secure systems against modern threats that bypass traditional controls; exploit known, unknown, or undisclosed vulnerabilities; either steal or encrypt personally identifiable data; or conduct malicious cryptocurrency mining. Smart, optimized, and connected, XGen security powers Trend Micro's suite.

Indicators of Compromise

Malware	SHA256
URSNIF	9d38a0220b2dfb353fc34d03079f2ba2c7de1d4a234f6a2b06365bfc1870cd89
DRIDEX	cbd130b4b714c9bb0a62e45b2e07f3ab20a6db3abd1899aa3ec21f402d25779e
EMOTET	0a47f5b274e803754ce84ebd66599eb35795fb851f55062ff042e73e2b9d5763
BitPaymer	d693c33dd550529f3634e3c7e53d82df70c9d4fbd0c339dbc1849ada9e539ea2

Related Posts:

- **Exploring Emotet: Examining Emotet's Activities, Infrastructure**
- **Monero-Mining RETADUP Worm Goes Polymorphic, Gets an AutoHotKey Variant**
- **IQY and PowerShell Abused by Spam Campaign to Infect Users in Japan with BEBLOH and URSNIF**
- **Phishing Campaign uses Hijacked Emails to Deliver URSNIF by Replying to Ongoing Threads**

Tags: BitPaymerDRIDEXEMOTETURSNIF

1 Comment TrendLabs 1 Login

♡ Recommend Tweet Share Sort by Best

Join the discussion…

LOG IN WITH

OR SIGN UP WITH DISQUS ?

Name

ali amair • a day ago

Can we also have SHA1 for these files as currently we dont have option in TMCM to add SHA256 under "User define objects"

^ | ˅ • Reply • Share ›

Subscribe Add Disqus to your siteAdd DisqusAdd Disqus' Privacy PolicyPrivacy PolicyPrivacy

Featured Stories

- systemd Vulnerability Leads to Denial of Service on Linux
- qkG Filecoder: Self-Replicating, Document-Encrypting Ransomware
- Mitigating CVE-2017-5689, an Intel Management Engine Vulnerability
- A Closer Look at North Korea's Internet
- From Cybercrime to Cyberpropaganda

Security Predictions for 2019

- Our security predictions for 2019 are based on our experts' analysis of the progress of current and emerging technologies, user behavior, and market trends, and their impact on the threat landscape. We have categorized them according to the main areas that are likely to be affected, given the sprawling nature of the technological and sociopolitical changes under consideration.
  Read our security predictions for 2019.

Business Process Compromise

- Attackers are starting to invest in long-term operations that target specific processes enterprises rely on. They scout for vulnerable practices, susceptible systems and operational loopholes that they can leverage or abuse. To learn more, read our Security 101: Business Process Compromise.

Recent Posts

- Android Wallpaper Apps Found Running Ad Fraud Scheme
- URSNIF, EMOTET, DRIDEX and BitPaymer Gangs Linked by a Similar Loader
- Cybercriminals Use Malicious Memes that Communicate with Malware
- Tildeb: Analyzing the 18-year-old Implant from the Shadow Brokers' Leak
- Cryptocurrency Miner Spreads via Old Vulnerabilities on Elasticsearch

Popular Posts

December Patch Tuesday: Year-End Batch Addresses Win32k Elevation of Privilege and Windows DNS Server Vulnerabilities
Fake Banking App Found on Google Play Used in SMiShing Scheme
Exploring Emotet: Examining Emotet's Activities, Infrastructure
Cryptocurrency Miner Spreads via Old Vulnerabilities on Elasticsearch

TrickBot’s Bigger Bag of Tricks

Stay Updated

Email Subscription

Your email here

Subscribe

- Home and Home Office
- |
- For Business
- |
- Security Intelligence
- |
- About Trend Micro

- Asia Pacific Region (APAC): Australia / New Zealand, 中国, 日本, 대한민국, 台灣
- Latin America Region (LAR): Brasil, México
- North America Region (NABU): United States, Canada
- Europe, Middle East, & Africa Region (EMEA): France, Deutschland / Österreich / Schweiz, Italia, Россия, España, United Kingdom / Ireland

- Privacy Statement
- Legal Policies