Taking Action Against Hackers in Bangladesh and Vietnam

about.fb.com/news/2020/12/taking-action-against-hackers-in-bangladesh-and-vietnam/

April 7, 2022

Today, we're sharing actions we took against two separate groups of hackers — APT32 in Vietnam and a group based in Bangladesh — removing their ability to use their infrastructure to abuse our platform, distribute malware and hack people's accounts across the internet.

Facebook's threat intelligence analysts and security experts work to find and stop a wide range of threats including malware campaigns, influence operations and hacking of our platform or individual Facebook accounts by nation state adversaries, hackers and others. As part of these efforts, our teams routinely disrupt adversary operations by disabling them, notifying users if they should take steps to protect their accounts, sharing our findings publicly and continuing to improve the security of our products.

Today we're sharing our latest research and enforcement actions against attempts to compromise people's accounts and gain access to their information, commonly referred to as cyber espionage. These two unconnected groups targeted people on our platform and elsewhere on the internet using very different tactics. The operation from Vietnam focused primarily on spreading malware to its targets, whereas the operation from Bangladesh focused on compromising accounts across platforms and coordinating reporting to get targeted accounts and Pages removed from Facebook.

The people behind these operations are persistent adversaries, and we expect them to evolve their tactics. However, our detection systems and threat investigators, as well as other teams in the security community, keep improving to make it harder for them to remain undetected. We will continue to share our findings whenever possible so people are aware of the threats we are seeing and can take steps to strengthen the security of their accounts.

Here's What We Found

Bangladesh

The Bangladesh-based group targeted local activists, journalists and religious minorities, including those living abroad, to compromise their accounts and have some of them disabled by Facebook for violating our Community Standards. Our investigation linked this activity to two non-profit organizations in Bangladesh: Don's Team (also known as Defense of Nation) and the Crime Research and Analysis Foundation (CRAF). They appeared to be operating across a number of internet services.

Don's Team and CRAF collaborated to report people on Facebook for fictitious violations of our Community Standards, including alleged impersonation, intellectual property infringements, nudity and terrorism. They also hacked people's accounts and Pages, and used some of these compromised accounts for their own operational purposes, including to amplify their content. On at least one occasion, after a Page admin's account was compromised, they removed the remaining admins to take over and disable the Page. Our investigation suggests that these targeted hacking attempts were likely carried out through a number of off-platform tactics including email and device compromise and abuse of our account recovery process.

To disrupt this activity, we removed the accounts and Pages behind this operation. We shared information about this group with our industry partners so they too can detect and stop this activity. We encourage people to remain vigilant and take steps to protect their accounts, avoid clicking on suspicious links and downloading software from untrusted sources that can compromise their devices and information stored on them.

Vietnam

APT32, an advanced persistent threat actor based in Vietnam, targeted Vietnamese human rights activists locally and abroad, various foreign governments including those in Laos and Cambodia, non-governmental organizations, news agencies and a number of businesses across information technology, hospitality, agriculture and commodities, hospitals, retail, the auto industry, and mobile services with malware. Our investigation linked this activity to CyberOne Group, an IT company in Vietnam (also known as CyberOne Security, CyberOne Technologies, Hành Tinh Company Limited, Planet and Diacauso).

As our industry partners have previously reported, APT32 has deployed a wide range of adversarial tactics across the internet. We have been tracking and taking action against this group for several years. Our most recent investigation analyzed a number of notable tactics, techniques and procedures (TTPs) including:

- **Social engineering:** APT32 created fictitious personas across the internet posing as activists and business entities, or used romantic lures when contacting people they targeted. These efforts often involved creating backstops for these fake personas and fake organizations on other internet services so they appear more legitimate and can withstand scrutiny, including by security researchers. Some of their Pages were designed to lure particular followers for later phishing and malware targeting.
- **Malicious Play Store apps:** In addition to using Pages, APT32 lured targets to download Android applications through Google Play Store that had a wide range of permissions to allow broad surveillance of peoples' devices.
- **Malware propagation:** APT32 compromised websites and created their own to include obfuscated malicious javascript as part of their watering hole attack to track targets' browser information. A watering hole attack is when hackers infect websites frequently visited by intended targets to compromise their devices. As part of this, the group built custom malware capable of detecting the type of operating system a target uses (Windows or Mac) before sending a tailored payload that executes the malicious code. Consistent with this group's past activity, APT32 also used links to file-sharing services where they hosted malicious files for targets to click and download. Most recently, they used shortened links to deliver malware. Finally, the group relied on Dynamic-Link Library (DLL) side-loading attacks in Microsoft Windows applications. They developed malicious files in *exe, rar, rtf* and *iso* formats, and delivered benign Word documents containing malicious links in text.

The latest activity we investigated and disrupted has the hallmarks of a well-resourced and persistent operation focusing on many targets at once, while obfuscating their origin. We shared our findings including YARA rules and malware signatures with our industry peers so they too can detect and stop this activity. To disrupt this operation, we blocked associated domains from being posted on our platform, removed the group's accounts and notified people who we believe were targeted by APT32.

Threat Indicators:

Hashes

```
768510fa9eb807bba9c3dcb3c7f87b771e20fa3d81247539e9ea4349205e39eb
69730f2c2bb9668a17f8dfa1f1523e0e1e997ba98f027ce98f5cbaa869347383
```

Domains

```
tocaoonline[.]com
qh2020[.]org
tinmoivietnam[.]com
nhansudaihoi13[.]org
chatluongvacuocsong[.]vn
tocaoonline[.]org
facebookdeck[.]com
thundernews[.]org
```

YARA Signatures

rule APT32_goopdate_installer

```
rule APT32_goopdate_installer {
  meta:
    reference = “https://about.fb.com/news/2020/12/taking-action-against-hackers-in-
bangladesh-and-vietnam/”
    author = “Facebook”
    description = "Detects APT32 installer side-loaded with goopdate.dll"
    sample = "69730f2c2bb9668a17f8dfa1f1523e0e1e997ba98f027ce98f5cbaa869347383"
  strings:
    $s0 = { 68 ?? ?? ?? ?? 57 A3 ?? ?? ?? ?? FF D6 33 05 ?? ?? ?? ?? }
    $s1 = "GetProcAddress"
    $s2 = { 8B 4D FC ?? ?? 0F B6 51 0C ?? ?? 8B 4D F0 0F B6 1C 01 33 DA }
    $s3 = "FindNextFileW"
    $s4 = "Process32NextW"

  condition:
    (pe.is_64bit() or pe.is_32bit()) and
    all of them
}
```

rule APT32_osx_backdoor_loader

```
rule APT32_osx_backdoor_loader {
  meta:
    reference = “https://about.fb.com/news/2020/12/taking-action-against-hackers-in-bangladesh-and-vietnam/”
    author = “Facebook”
    description = "Detects APT32 backdoor loader on OSX"
    sample = "768510fa9eb807bba9c3dcb3c7f87b771e20fa3d81247539e9ea4349205e39eb"
  strings:
    $a1 = { 00 D2 44 8A 04 0F 44 88 C0 C0 E8 07 08 D0 88 44 0F FF 48 FF C1 48 83 F9 10 44 88 C2 }
    $a2 = { 41 0F 10 04 07 0F 57 84 05 A0 FE FF FF 41 0F 11 04 07 48 83 C0 10 48 83 F8 10 75 }

    // Encrypted data
    $e1 = { CA CF 3E F2 DA 43 E6 D1  D5 6C D4 23 3A AE F1 B2 } // Decoded to drop filepath: '/tmp/panels'
    $e2 = "MlkHVdRbOkra9s+G65MAoLga340t3+zj/u8LPfP3hig=" // Decoded to export API name 'ArchaeologistCodeine'
    $e3 = { 5A 69 98 0E 6C 4B 5C 69  7E 19 34 3B C3 07 CA 13 } // Decoded to 'ifconfig -l'
    $e4 = "1Sib4HfPuRQjpxIpECnxxTPiu3FXOFAHMx/+9MEVv9M+h1ngV7T5WUP3b0zsg0Qd" // Decoded to export API 'PlayerAberadurtheIncomprehensible'

    // Decoded export func names
    $e5 = "_ArchaeologistCodeine"
    $e6 = "_PlayerAberadurtheIncomprehensible"

  condition:
    ((uint32(0) == 0xfeedface or uint32be(0) == 0xfeedface) or (uint32(0) == 0xfeedfacf or uint32be(0) == 0xfeedfacf)) and
   (
      2 of ($e*) or
      all of ($a*)
   )
}
```