Anomali Suspects that China-Backed APT Pirate Panda May Be Seeking Access to Vietnam Government Data Center

anomali.com/blog/anomali-suspects-that-china-backed-apt-pirate-panda-may-be-seeking-access-to-vietnam-government-data-center

Research | April 30, 2020

by Anomali Threat Research

Authored by: Sara Moore, Joakim Kennedy, Parthiban R, and Rory Gould

The Anomali Threat Research Team detected a spear phishing email targeting government employees in the Municipality of Da Nang, Vietnam. The email contained a malicious Microsoft Excel document which drops a malicious Dynamic-Link Library (DLL) providing the actor with CMD reverse shell over HTTP. The DLL shares code similarities to exile-RAT, a tool associated with Pirate Panda. Pirate Panda is an APT backed by China and known for targeting government and political organisations.

Pirate Panda has reportedly focused primarily on issues surrounding territorial conflicts in the South China Sea [1]. As Da Nang lies on the Coast of Vietnam, opposite the Paracel Islands (an area of territorial dispute), this may provide some understanding of why Pirate Panda would consider targeting this municipality. [2]

The phishing email and lure document observed suggest that the employees targeted likely work within a government-run data center. Such attacks are consistent with other regional APT campaigns [3]. If Pirate Panda were to compromise a government-run data center, it would have access to vast amounts of sensitive information.

Targeted Phishing

In the screenshot below, the phishing email shown was sent by a government employee to another government employee. The intended victim had a “danang.gov.vn” appended to the email address, as seen in the email headers.

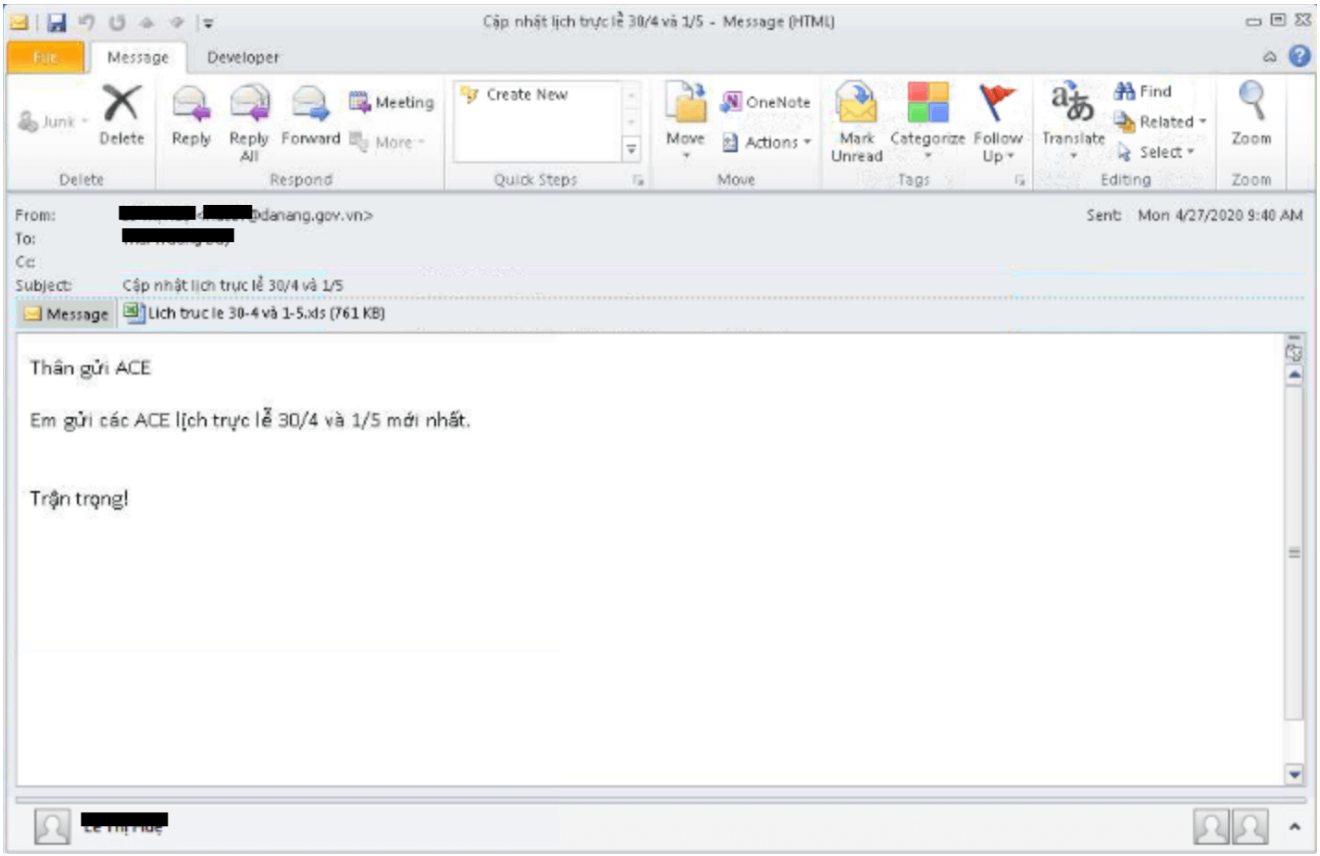

Figure 1, Phishing email

The subject header is “Cập nhật lịch trực lễ 30/4 và ⅕,” which Google translates as “Updated live schedule 30_4 and 1_5.eml.” The live schedule appeared to be for the dates of April 30 and May 1, which may indicate that the lure theme was related to events on those days. As both 30 April and 1 May are Vietnamese national holidays, it is plausible the theme related to those events, although we cannot confirm that hypothesis based on available data.

- 30 April is “Reunification Day,” marking the unification between North and South Vietnam in 1975
- May is Vietnam’s national “Labour Day” holiday, which has political associations with communism and the working class

```
X-Account-Key: account5
X-UIDL: 1674
X-Mozilla-Status: 0001
X-Mozilla-Status2: 00000000
X-Mozilla-Keys:
Received: from MBX01.DSP-INT.VN (10.196.132.154) by MBX01.DSP-INT.VN
(10.196.132.154) with Microsoft SMTP Server (TLS) id 15.0.1497.2 via Mailbox
Transport
Mon, 27 Apr 2020 16:40:20 +0700
Received: from MBX02.DSP-INT.VN (10.196.132.155) by MBX01.DSP-INT.VN
(10.196.132.154) with Microsoft SMTP Server (TLS) id 15.0.1497.2
Mon, 27 Apr
2020 16:40:18 +0700
Received: from MBX02.DSP-INT.VN ([fe80::9575:56d1:dc0:b32]) by
MBX02.DSP-INT.VN ([fe80::9575:56d1:dc0:b32%16]) with mapi id 15.00.1497.000
Mon, 27 Apr 2020 16:40:18 +0700
From: =
TMOqIFRo4buLIEh14buH
= <[redacted]@danang.gov.vn>
VGjDoWkgVHLGsOG7nW5nIER1eQ==
= <[redacted]@danang.gov.vn>
Subject:
Q+G6rXAgbmjhuq10IGzhu4tjaCB0cuG7sWMgbOG7hSAzMC80IHbDoCAxLzU=
Thread-Topic:
Thread-Index: AQHWHHdBbMyrzsMQjE6294gNy74xSg==
Date: Mon, 27 Apr 2020 16:40:18 +0700
Message-ID: <1587980609169.73222@danang.gov.vn>
Accept-Language: vi-VN, en-US
Content-Language: vi-VN
X-MS-Exchange-Organization-AuthAs: Internal
X-MS-Exchange-Organization-AuthMechanism: 04
X-MS-Exchange-Organization-AuthSource: MBX02.DSP-INT.VN
X-MS-Has-Attach: yes
```

Figure 2, Email header for phishing sample

We assess that the phishing email likely came from a genuine internal mailbox, as Microsoft Exchange categorised it as “Internal” and the IP address in the email header 10.196.132.154 was from an internal private network. If the originating email account was associated with a real employee, that employee was likely compromised previously, or they are conducting internal pentesting.

An open-source search of both email addresses only located information about the victim email address in an online spreadsheet titled “Công viên phần mềm Đà Nẵng,” which Google translates to “Da Nang Software Park.” We were unable to determine what if any link exists between the government employees listed and the park. The spreadsheet contained email addresses, telephone numbers and possible job titles for Da Nang government employees, with the victim’s job title translating to “Expert”. The

spreadsheet was hosted on dsp.vn, a government-owned site that described the Da Nang IT Infrastructure Development Center as having been established under the People's Committee of Da Nang City, a non-business unit under the Department of Information and Danang media. [4]

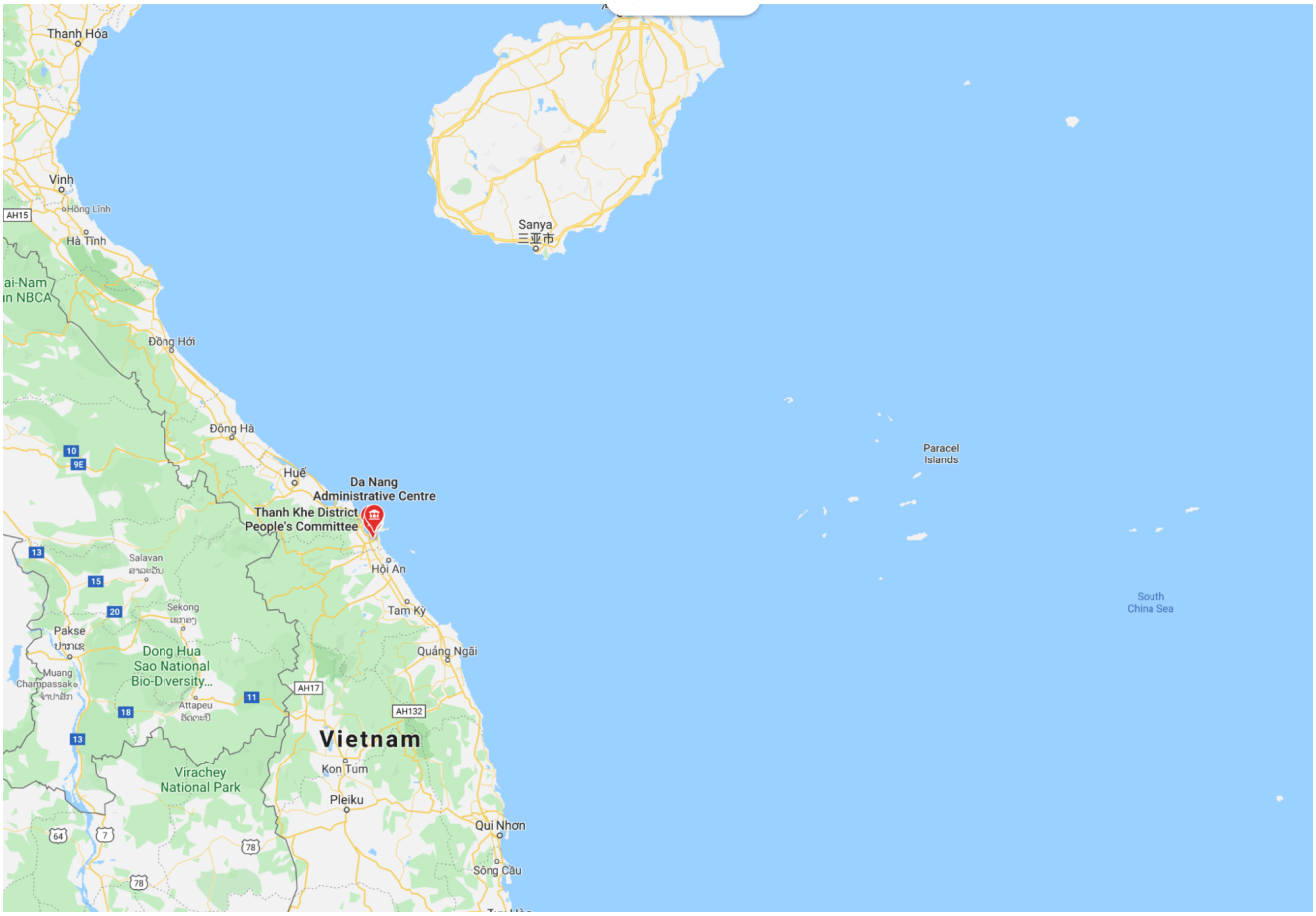

Figure 3, location of Da Nang

Da Nang lies on the coast across from the Paracel Islands, an area of territorial dispute [5]. in March 2020, the USS Theodore Roosevelt visited the port of Da Nang to commemorate the relationship between Vietnam and the United States [6]. According to press reporting, ”Washington has placed a high priority on improving its defense ties with Vietnam recently as part of President Donald Trump’s National Defense Strategy, which prioritizes strategic competition with China and countering its growing military capabilities in Asia.” [7]

Since the outbreak of COVID-19, there has been an increase in naval activity in the South China Sea, including the Chinese aircraft carrier Liaoning and US Navy ships patrolling the area; indications of ongoing regional tensions.

Malicious Excel Document

The phishing email contains an attachment called “lich truc li,” which translates as “office schedule.”

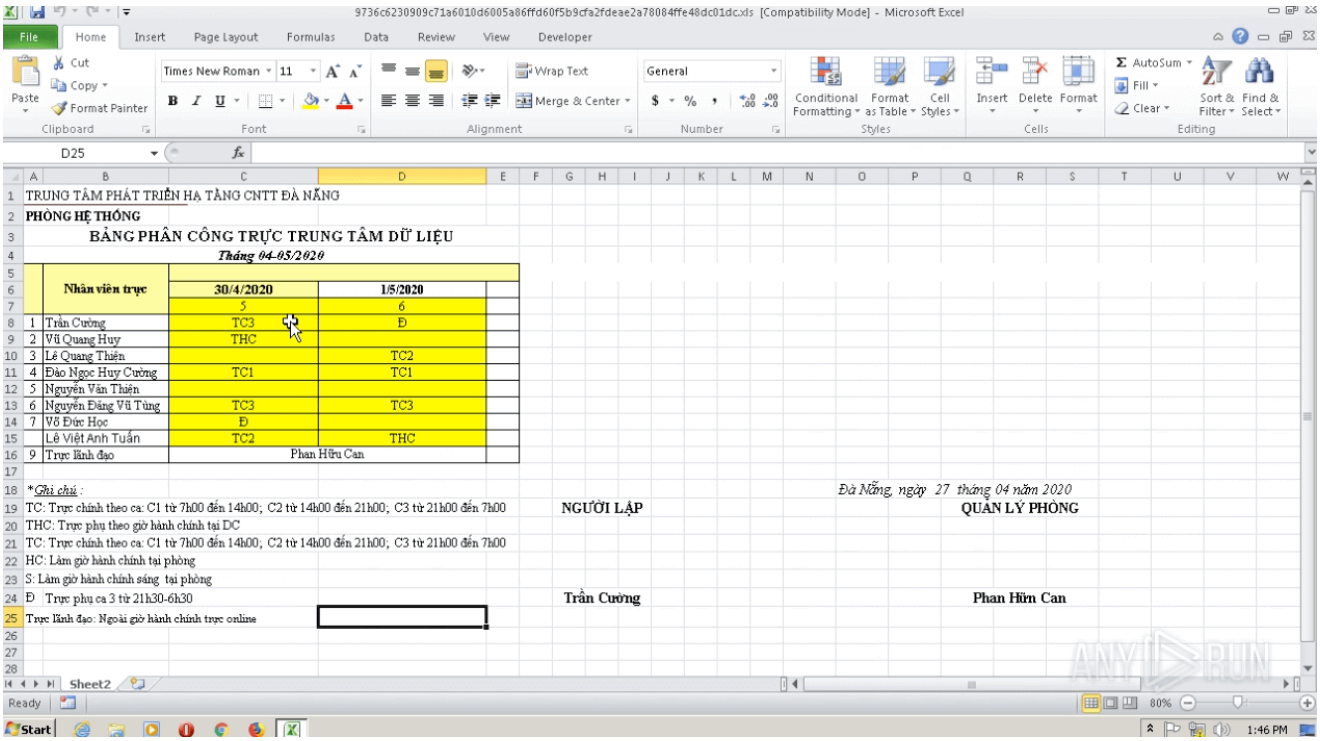

Figure 4, Screenshot of the malicious excel document

The spreadsheet contained a table with three titles “bảng phân công trực trung tâm dữ liệu,” which translates as “Data Center assignment table,” “TRUNG TÂM PHÁT TRIỂN HẠ TẦNG ĐA NĂNG,” which translates as “Multi-infrastructure development center,” and “phòng hệ thống,” which translates as “system room.” This may support a hypothesis that the government employees work in a data center in the Da Nang Software Park. This spreadsheet is likely an employee schedule. Column B appears to hold employee names, whilst C & D correspond with shift patterns laid out in rows 19-24. An open-source search suggests that the acronyms "“TC1,” “TC2,” and “TC3” may refer to technology centers.

When the Excel document is opened, two executables (utilman.exe and mpsvc.dll) will be dropped at folder %AppData%MicrosoftCorporation. Utilman.exe is Windows Defender executable MsMpeng.exe. The attacker is employing a DLL Side-Loading technique using a legitimate security product to load a malicious dll [8]. This is a common technique for a variety of threat actors and groups. A shortcut for utilman.exe is then created at the startup folder so that the dropped files execute during the next reboot of the machine and communicate with a command and control (C2).

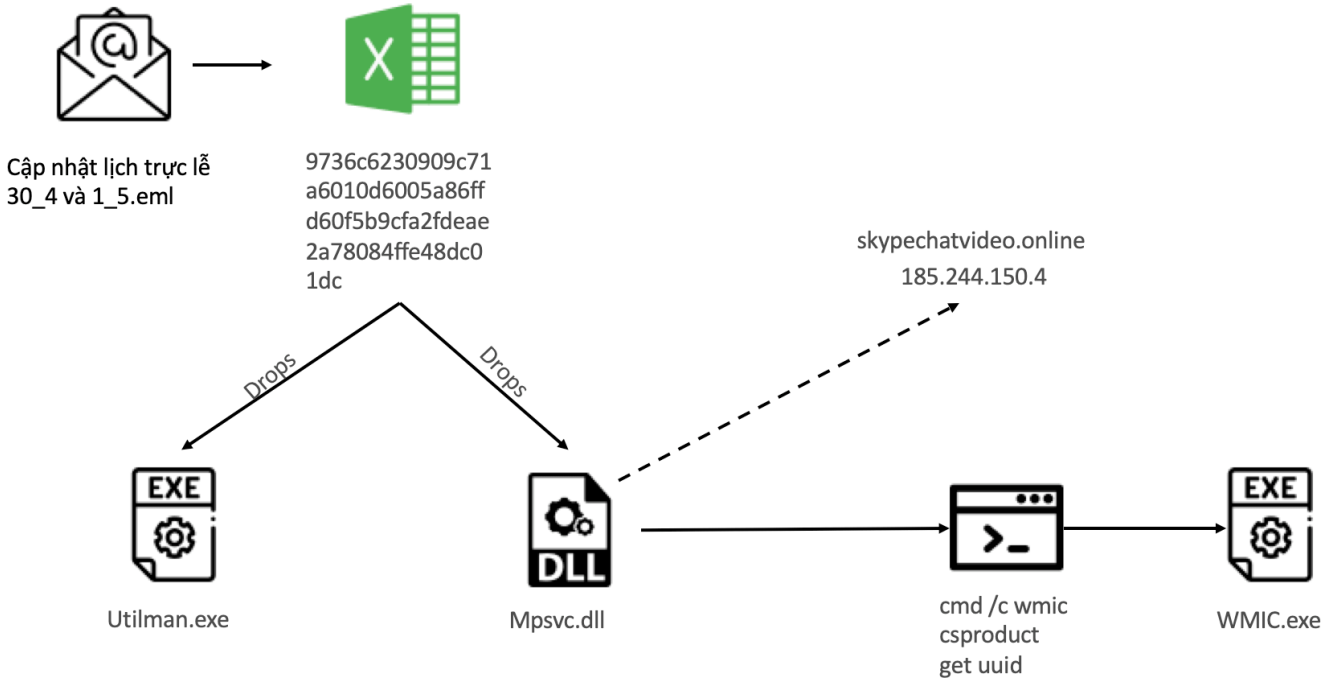

Figure 5, process graph

Mpsvc.dll initially makes a number of DNS requests to “dns.google” (8.8.8.8 and 8.8.4.4) which is Google’s public DNS service. The domain name resolved as skypechatvideo[.]online.

	380	49.699831	192.168.100.38	8.8.8.8	SSLv2	90 Client Hello
	381	49.740506	8.8.8.8	192.168.100.38	TCP	54 443 → 49900 [ACK] Seq=1 Ack=37 Win=64256 Len=0
	382	49.756918	8.8.8.8	192.168.100.38	TLSv1	61 Alert (Level: Fatal, Description: Protocol Version)
	383	49.756947	8.8.8.8	192.168.100.38	TCP	54 443 → 49900 [FIN, ACK] Seq=8 Ack=37 Win=64256 Len=0
	384	49.757086	192.168.100.38	8.8.8.8	TCP	54 49900 → 443 [ACK] Seq=37 Ack=9 Win=66304 Len=0
	385	49.757434	192.168.100.38	8.8.8.8	TCP	54 49900 → 443 [FIN, ACK] Seq=37 Ack=9 Win=66304 Len=0
	386	49.798973	8.8.8.8	192.168.100.38	TCP	54 443 → 49900 [ACK] Seq=9 Ack=38 Win=64256 Len=0
	395	51.327219	192.168.100.38	185.244.150.4	TCP	66 49927 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_P…
	397	51.370485	185.244.150.4	192.168.100.38	TCP	66 80 → 49927 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1206 S…
	398	51.370745	192.168.100.38	185.244.150.4	TCP	54 49927 → 80 [ACK] Seq=1 Ack=1 Win=66304 Len=0
	399	51.371041	192.168.100.38	185.244.150.4	HTTP	298 GET /wwwlib/title.php?ID=NzhERjJFQjgtNDk5RC03ODQ0LTlCNzctM0U…
	400	51.411267	185.244.150.4	192.168.100.38	TCP	54 80 → 49927 [ACK] Seq=1 Ack=245 Win=64128 Len=0

Figure 6, pcap file for mpsvc.dll

After communicating to Google DNS, the victim machine communicates with the C2 skypechatvideo[.]online and sends the following GET request:

http://skypechatvideo[.]online/wwwlib/title.php?
ID=NzhERjJFQjgtNDk5RC03ODQ0LTlCNzctM0U2QUVBREYyNEU4:U1Q=

The C2 was hosted on an Apache server running PHP, and communicated with the victim machine over port 49927. The domain skypechatvideo[.]online, which was registered at IP address 185.244.150[.]4 on April 20, 2020 with Registrar NameSilo, was using a privacy service that obfuscated the registrant information. Additionally, according to RiskIQ, only one other domain hosted on the IP address 185.244.150[.]4: onlinedocumentviewer[.]us which was first seen in July 2018. The small number of domains suggests the infrastructure is owned rather than shared, and the long period between the domains makes the relationship between them questionable.

The dropped executable mpsvc.dll, although containing a large quantity of unique code, was genetically similar to exile-RAT and keyboy; both are RATs Pirate Panda deploys. It is likely that the threat actors modified and developed the code since it was last used. The dll has a compilation date of 22 April 2020,

which is two days after the c2 domain was registered, and the phishing email was sent on 27 April 2020. exile-RAT has been observed using the same DLL Sideloading technique, using a legitimate security product to load a malicious dll. In this instance, Windows Defender is being used.

Conclusion

The phishing email and the lure document suggest that the attack was crafted to target government employees working at a data centre, which is consistent with previous data center targeting by other campaigns attributed to APTs [9]. If the phishing email was sent by a real employee, it is possible that members of the Da Nang government have already been compromised, but were not the targets of interest or didn't have the required access to desired information. It is possible that the national holidays are being used as a lure, because the threat actors may have an imminent desire for lateral movement and access to data. While Anomali has not been able to figure out what information the threat actors are attempting to obtain, if an attacker were to compromise a government-run data center, it would have access to vast amounts of sensitive information. Read more about People's Republic of China (PRC) in this cybersecurity profile.

How Anomali Helps

The Anomali Threat Research Team provides actionable threat intelligence that helps customers, partners, and the security community to detect and mitigate the most serious threats to their organizations. The team frequently publishes threat research in the form of white papers, blogs, and bulletins that are made available to the security community, general public, and news organizations. Intelligence and bulletins about threat actors and related Indicators of Compromise (IOCs) are integrated directly into Anomali Altitude customers' security infrastructures to enable faster and more automated detection, blocking, and response. For more information on how Anomali customers gain integrated access to threat research, visit: https://www.anomali.com/products.

Endnotes

[1] CrowdStrike, "CrowdStrike: Ongoing Pirate Panda operations using current event themes", published March 2nd 2020, accessed April 29th 2020, https://www.scribd.com/document/451284814/CrowdStrike-Ongoing-Pirate-Panda-operations-using-current-event-themes.

[2] Minnie Chan, "Chinese military lashes out at American warship's 'intrusion' in South China Sea", South China Morning Post, published April 28th 2020, accessed April 28th 2020, https://www.scmp.com/news/china/diplomacy/article/3081970/chinese-military-lashes-out-american-warships-intrusion-south.

[3] Denis Legezo, "Chinese Cyber-Espionage Group Hacked Government Data Center", Kasperksy, published June 15th 2018, accessed April 28th 2020, https://securelist.com/luckymouse-hits-national-data-center/86083/.

[4] General Administrative Office, "Da Nang IT Infrastructure Development Center", published November 23rd 2017, accessed April 28th 2020, https://dsp.vn/chi_tiet-6420.

[5] Minnie Chan, "Chinese military lashes out at American warship's 'intrusion' in South China Sea", South China Morning Post, published April 28th 2020, accessed April 28th 2020, https://www.scmp.com/news/china/diplomacy/article/3081970/chinese-military-lashes-out-american-warships-intrusion-south.

[6] U.S. Embassy and Consulate in Vietnam, “Theodore Roosevelt Strike Group Completes Port Visit to Da Nang to Commemorate 25 Years of Diplomatic Relations“, published March 11th 2020, accessed April 28 2020, https://vn.usembassy.gov/theodore-roosevelt-strike-group-completes-port-visit-to-da-nang-to-commemorate-25-years-of-diplomatic-relations/.

[7] Benjamin Wilhelm, “Could China’s Aggression in the South China Sea Boost U.S.-Vietnam Relations?”, World Politics Review, published April 8th 2020, accessed April 28th 2020, https://www.worldpoliticsreview.com/trend-lines/28669/could-china-s-aggression-in-the-south-china-sea-boost-u-s-vietnam-relations.

[8] Marcus Pietro, “DLL Side-Loading for Fun (and Profit?) - Day 4”, Marpie , published January 4th 2019, accessed April 28th 2020, https://www.a12d404.net/security/2019/01/04/side-loading-fun-4.html.

[9] Denis Legezo, “Chinese Cyber-Espionage Group Hacked Government Data Center“, Kasperksy, published June 15th 2018, accessed April 28th 2020, https://securelist.com/luckymouse-hits-national-data-center/86083/.

Appendix A: Indicators of Compromise (IOCs)

Indicator of Compromise	Description
cd075ddb7cbe9bfb9ca955be605a6f622d83bcef7eded2b495c653e86fe9b59e	Phishing Email Sample
9736c6230909c71a6010d6005a86ffd60f5b9cfa2fdeae2a78084ffe48dc01dc	Excel document lure sample
80C3E22B640B47E0C41F4185F091E2C523A9EF291A75B7007303E2267B8D68C5	Utilman.exe - MsMpEng.exe which is Windows Defender (legitimate security tool)
A369FEE3B83C2D2534C48FDFAC8D03A266809AAA28ACE6B6002EAB57CC14EDD1	Mpsvc.dll - malicious DLL
skypechatvideo[.]online	C&C Domain

Topics: Research