Updated 1-11-20

ACS Advanced Cyber Security Corp.

Below is a list of stories and breaches implicating keylogging spyware

KEYLOGGERS IN THE NEWS

January 11, 2021

RESEARCHERS FIND LINK BETWEEN SUNBURST AND RUSSIAN KAZUAR MALWARE

Cybersecurity researchers, for the first time, may have found a potential connection between the backdoor used in the SolarWinds hack to a previously known malware strain. In new research published by Kaspersky researchers today, the cybersecurity firm said it discovered several features that overlap with another backdoor known as Kazuar, a .NET-based malware first documented by Palo Alto Networks in 2017. On November 18, 2020, Kazuar appears to have undergone a complete redesign with a new keylogger and password-stealing functions added to the backdoor that's implemented in the form of C2 server command.

January 5, 2021

HACKERS TARGET CRYPTOCURRENCY USERS WITH NEW ELECTRORAT MALWARE

ElectroRAT has various capabilities such as keylogging, taking screenshots, uploading files from disk, downloading files, and executing commands on the victim's console.

December 29, 2020

HOW TO DETECT A KEYLOGGER ON ANDROID

Hackers can install a keylogger on your smartphone silently or remotely and it will grab all of your data from your smartphone. Such as text messages, call logs, save notes, browsing details, passwords, etc.

December 28, 2020

NZBGEEK HAS BEEN HACKED LEAVING PRIVAATE DATA EXPOSED

According to the site’s operators, the hackers were able to put a keylogger on the site and also managed to get a copy of the database. The compromised data includes user emails and encrypted passwords.

December 10, 2020

APT GROUP TARGETING EAST ASIAN GOVERNMENT AGENCIES

For this attack, he indeed associated keyloggers with backdoors to upload various tools capable of analyzing the target's network, in order to recover identification data. These tools have also given hackers access to sensitive government data.

November 16, 2020

CYBERCRIME MOVES TO THE CLOUD TO ACCELERATE ATTACKS AMID DATA GLUT

Cybercriminals are embracing cloud-based services and technologies in order to accelerate their attacks on organizations and better monetize their wares, researchers have found. This is largely driven by cybercriminals who sell access to what they call “clouds of logs,” which are caches of stolen credentials and other data hosted in the cloud.

Malicious actors are turning to the cloud in order to work more effectively with the sheer volume of data on offer in underground forums, researchers said.

“In recent years, the theft of user credentials has been on the rise, with attackers collecting massive amounts of credentials and associated email addresses or domain names,” researchers explained. “[Other data stolen] often includes recorded keystrokes, authentication credentials to online portals, online banks, authenticated session attributes, personally identifiable information (PII), scans of documents, tax reports, invoices, bank account payment details (for example, credit cards), and more.”

November 16, 2020

WHAT ARE THE 5 MAJOR CYBERSECURITY MISTAKES I CAN AVOID AS A SMALL BUSINESS OWNER

Many of these types of malware are delivered to you or your employees through phishing expeditions or Trojan horses. A phishing attack usually comes in the shape of an authentic-looking email to your company and carries fraudulent links or malware. Meanwhile, Trojan horses are malware disguised as legitimate software.

Mistake #1: Underestimating Cybersecurity Threats:

- **Keyloggers** are a sneaky type of spyware that log your keystrokes and send them to hackers to help them commit financial fraud.

November 13, 2020

WHY WAS MY FACEBOOK ACCOUNT HACKED?

Keylogging is another common tactic for hackers. A keylogger program, which can be set up on your device remotely, records the keys you enter. Key-loggers can record your password information or even your banking information.

November 4, 2020

NORTH KOREAN MALWARE TARGETING GOVERNMENT AGENCIES

Organizations that were targeted include government and defense organizations, journalists, human rights groups, and pharmaceutical and research companies working on COVID-19 therapies. The researchers discovered that KGH_SPY is a modular suite of tools that provides the threat actors with reconnaissance, keylogging, information stealing, and backdoor capabilities and that CSPY Downloader is designed to evade analysis and download additional payloads.

October 22, 2020

TRUMP AND BIDEN MOBILE APP VULNERABILITIES RAISE CONCERN

And finally, both apps allow third-party keyboards to be used. Custom keyboards observe user input and can potentially record/export the collected data via keylogging.

October 2, 2020

NY: FORMER INFORMATION TECHNOLOGY EMPLOYEE OF HOSPITAL SENTENCED TO 30 MONTHS IN PRISON FOR COMPUTER INTRUSION

RICHARD LIRIANO was sentenced yesterday to 30 months in prison for engaging in a scheme to use malicious software programs, including a program known as a "keylogger," on dozens of his coworkers' computers at a New York City-area hospital, secretly obtaining user names and passwords to his victims' personal email and other accounts, and using that unauthorized access to steal private and confidential files. Using his victims' stolen credentials, LIRIANO repeatedly compromised their password-protected online accounts, and accessed their sensitive personal photographs, videos, and other private documents. LIRIANO's computer intrusions into Hospital-1's computer networks caused over $350,000 in losses to Hospital-1, which include the expenses that Hospital-1 incurred to remediate the damage that LIRIANO caused to its computer networks.

September 25, 2020

NEW MALWARE ALIEN THAT CAN STEAL CREDENTIALS FROM 226 ANDROID APPS

The malware can leverage its keylogger for any use and, therefore, broaden the attack scope further than its target list.

September, 09, 2020

AUGUST 2020'S MOST WANTED MALWARE:

- Agent Tesla is an advanced RAT functioning as a keylogger and information stealer, capable of monitoring and collecting the victim's keyboard input
- Formbook is an Info Stealer that harvests credentials from various web browsers, collects screenshots, monitors and logs keystrokes, and can download and execute files according to its C&C orders.

August 19, 2020

WHAT IS A KEYLOGGER? EVERYTHING YOU NEED TO KNOW

Keylogging is a way to spy on a computer user. It's generally used to gain access to passwords and other confidential information through fraud. It records every keystroke made on your computer. Your mobile device can also get infected in the same way as a computer – via phishing emails and malicious websites.

- Over the past 10 years, IT security companies have recorded a steady increase in keylogger-based malware.
- However, 80% of all keyloggers are not detectable by antivirus software or firewalls.

June 30, 2020

THEIFQUEST RANSOMWARE ENCRYPTS MACOS SYSTEMS BUT ALSO INSTALLS A KEYLOGGER AND A REVERSE SHELL FOR FULL CONTROL OVER INFECTED HOSTS

Armed with these capabilities, the attacker can main full control over an infected host," said Patrick Wardle, Principal Security Researcher at Jamf. This means that even if victims paid, the attacker would still have access to their computer and continue to steal files and keyboard strokes.

June 15, 2020

THIS DANGEROUS NEW KEYLOGGER COULD CHANGE THE ENTIRE MALWARE SPACE

Keyloggers make up the largest volume of unique phishing campaigns unique by malware type today and they continue to grow in both popularity and sophistication.The reason that Cofense is so concerned about MassLogger keylogger is due to how quickly the malware is updated. Its author consistently updates and improves Mass Logger and this allows cybercriminals deploying the malware to overcome security measures taken to detect and defend against it.

May 12, 2020

WHAT IS DRIDEX?

Dridex (also known as Bugat and Cridex) is a malicious program that is used to steal banking credentials from users of Windows computers. Cyber criminals proliferate this rogue software when it is downloaded and installed through a malicious Microsoft Word or Excel document. The main goal of this malware is to steal sensitive details relating to victims' bank accounts, such as online banking credentials. Therefore, this malicious software helps distributors and cyber criminals to access victims' bank accounts and make fraudulent transactions - effectively stealing money from unsuspecting people. This malicious software operates as a keylogger and records keystrokes (keys pressed). Cyber criminals seek to infect computers with these key loggers so they can steal logins, passwords, and other sensitive details, including banking credentials. This program is also capable of performing several 'injection attacks'. These attacks allow injection of malware into a computer system to execute remote commands or inject code into a specific program and modify its execution/behavior.

May 8, 2020

SCAMS TO WATCH OUT FOR NOT JUST THIS MOTHER'S DAY

Once a bogus coupon tickles your fancy and you click on it, a malware installer can be downloaded on to your device; in some cases, it can turn out to be a banking trojan or even a keylogger.

April 15, 2020

KEYLOGGER DISGUISED AS FREE GAMING APP

Attackers are disguising malicious software that looks like a product licensing key that would grant a user access to the beta version of "Valorant," a new title from the developer Riot Games. However, the game-key generator actually includes keylogger software that would allow hackers to track the words and phrases that users type.

April 12, 2020

U.S. CORONAVIRUS PHISHING EMAILS INCREASE 32 TIMES

Researchers also noted that spyware turned out to be the most popular attachments in letters, with backdoors taking the second place. The most common spyware programs are AgentTesla, NetWire, and LokiBot.

March 20, 2020

WHO CHIEF EMAIL S CLAIMING TO OFFER CORONAVIRUS

Fraudsters are trying to capitalize on fears surrounding the virus in new phishing campaigns. Emails claiming to be from the leader of the World Health Organization (WHO) are making the rounds in new phishing campaigns designed to plant keyloggers on your PC.

March 20, 2020

REVAMPED HAWKEYE KEYLOGGER SWOOPS IN ON CORONAVIRUS FEARS

There's a new variant of the HawkEye keylogging malware making the rounds, featuring expanded info-stealing capabilities. Its operators are looking to capture the zeitgeist around the novel coronavirus. It's being distributed using spam that purports to be an "alert" from the Director-General of the World Health Organization (WHO).

March 10, 2020

SPAMMERS USE CORONAVIRUS MESSAGE TO DEPLOY KEYLOGGER

Hackers are weaponizing the COVID-2019 coronavirus disease, trying to trick people into downloading malware so attackers can steal valuable information from victims' computers. Security researchers observed the spread of a file named "CoronaVirusSafetyMeasures_pdf," most likely in the form of email attachments, which is actually a RAT dropper (remote access trojan) that acts as a keylogger, registering all key presses.

February 07, 2020

BANKING TROJAN EMPLOYS NEW TRICKS, EXPANDS CAMPAIGN STEALS USER'S PASSWORDS WITH THE HELP OF KEYLOGGING TRICK

Once the Trojan infects the system, it erases the auto-suggest and auto-complete information from all the browsers, making users re-type their passwords when trying to login to the online banking account. As a result, the password is stolen (by the keylogger) and sent to a remote server, which allows the threat actors to abuse the financial information by selling it online or using it to steal money directly.

January 14, 2020

NSA FOUND A DANGEROUS MICROSOFT FLAW AND ALERTED THE FIRM – RATHER THAN WEAPONIZING IT

A sophisticated hacker seeking to exploit the flaw could build a weapon that reroutes users to malicious sites, steals files, activates microphones, records keystrokes and passwords, wipes disks, installs ransomware, "you name it," said Jake Williams, a former NSA hacker who co-founded Rendition Infosec, a cybersecurity firm.

January 09, 2020

NEW BANKING HACK STEALS YOUR KEYSTROKES

Dark Tequila used keylogging, which steals every keystroke from a user's keyboard to gain access to passwords and other confidential information.

January 6, 2020

HOSPITAL EMPLOYEE PLEADS GUILTY TO FIVE YEAR ACCOUNT HACKING SPREE

The U.S. Department of Justice (DOJ) has announced that a former employee of a New York City hospital has pleaded guilty to using malicious software to obtain the credentials of coworkers, which he subsequently misused to steal sensitive information. “He used a keylogger to obtain the credentials of dozens of co-workers at the hospital between 2013 and 2018. Those credentials allowed Liriano to login to coworkers’ computers and online accounts and obtain sensitive information such as tax documents, personal photographs, videos, and other private documents and files.”

January 2, 2020

DOZENS OF HOSPITAL COMPUTERS COMPROMISED, FORMER EMPLOYEE PLEADS GUILTY

Richard Liriano, a former IT employee of a New York City-area hospital pled guilty of a computer fraud. He used a “keylogger” on dozens of his coworkers’ computers to obtain usernames and passwords of their personal email and other social media accounts. According to the (Department of Justice (DOJ), “Using the victims’ stolen credentials, Richard repeatedly compromised their password-protected online accounts, and accessed their sensitive personal photographs, videos, and other private documents.” The keylogger enabled him record computer user’s keystrokes.