HOW KEYLOGGERS WORK AND HOW TO DEFEAT THEM

Homeworking policies, necessary to curtail COVID-19, have also had the effect of exposing smaller enterprises to a level of sophisticated cyber-attack ordinarily reserved for large multi-nationals, writes Dave Waterson, CEO of SentryBay.

The pandemic has been widely exploited by malicious cyber actors and advanced persistent threat groups using COVID-19 themes, putting individuals, small and medium businesses and large organisations at risk of scams and phishing attacks. According to a report by the National Cyber Security Centre[1], they detected 723 incidents in the year to September 2020, of which 27% related to coronavirus.

The risk of attack is further exacerbated by the geographically widespread location of employees. Even as we sit out another nationwide lockdown, it is difficult to see how dispersed workforces will return to the office any time soon. The likelihood, conversely, is that more and more companies will endorse WFH as a policy for the future.

Less corporate control in home cyber security

The net result of this, is that sensitive company data has a broader physical footprint and organisations have less control over how it is being accessed if their employees are outside the safety of the corporate perimeter. Where smaller enterprises, which are often less stringently protected, were previously able to fly under the radar and avoid cyber-attacks, this is no longer the case. They are increasingly being hit with insidious, damaging breaches that they are ill-equipped to deal with in the current climate.

An Interpol assessment[2] of the impact of COVID-19 on cybercrime in August 2020, said 'The increased online dependency for people around the world is creating new opportunities, with many businesses and individuals not ensuring their cyber defences are up to date'. Alarmingly, Interpol also pointed out that with a COVID-19 vaccination available, it is highly probable that there will be another spike, particularly in phishing attacks, related to these medical products as well as network intrusion and cyberattacks to steal data.

Keyloggers and screen-grabbers are biggest threat

In 2021, we fully anticipate that the greatest danger to organisations and especially in smaller enterprises, will come from keylogging and screen-grabbing malware, primarily because they are the attack vector through which sensitive data is most often and most easily, stolen. Along with spyware, keylogging malware was ranked as the highest threat by the 2019 *Global Threat Intelligence Report*[3].

> "Along with spyware, keylogging malware was ranked as the highest threat by the 2019 Global Threat Intelligence Report."

Both forms of malware use endpoint devices to gain access to corporate networks and, despite the rise in use of anti-virus and two-factor authentication, this will not guard against an attack. In fact, with a keylogger installed on a remote endpoint laptop, which has a lower security posture than it would within the secure corporate perimeter, an attacker could have full access as the user logs in and to everything the user enters at the keyboard or displays in a local application.

It's wishful thinking at best to believe two-factor authentication will stop sensitive data passing through the application after login. Standard anti-virus solutions are also not equipped to provide enough protection. Unless data is protected as it is entered from the keyboard or onto the screen, it reveals a chink in the corporate armour to criminals who will not hesitate to strike.

To plan a security strategy that will protect today's newly distributed workforce and the companies they work for, it's important to think about where threats start and how they can be arrested.

Stop keyloggers executing undetected

Kernel-level keyloggers, the most dangerous form of keylogger attackers, harvest keys typed on the keyboard the moment they enter the operating system. These low-level keyloggers are notoriously difficult to identify and eliminate, hence their success against standard anti-virus solutions, so they often execute undetected.

What is effective against this threat are solutions operating at the kernel level, which specifically protect the data being entered without relying on identifying and eliminating keyloggers. These solutions bypass any installed kernel level keyloggers, feeding false random data into the system while ensuring the real keystrokes are safely delivered to the application. They operate regardless of whether a keylogger is present or not.

Data in the application

It is not only the login access which is vulnerable to threats: all data entered

Image: stock.adobe.com/ Martin

doi:10.1093/itnow/bwab017

into an application after login, or sensitive data displayed on the screen through the application, is also vulnerable. These attacks include screen capture or screen grabbing, DLL injection and man-in-the-browser (MITB) attacks. Screen grabbing malware is generally triggered to capture the screen upon certain events, such as the opening of a customer's account details, for example and this happens perhaps every five or ten seconds while the target application has focus.

The malware then covertly sends the captured screen images through to the command and control server of the attacker, where any data visually open on the image is stolen. Most companies are aware of the dangers of login credentials being stolen and advise their staff to use 2FA, select complex passwords and to update them regularly. However, screen grabbing, if it can be executed, puts all information held within applications, as well as all information entered at the keyboard, under threat.

Specific anti-screen capture methods can be employed to monitor and control screen capture APIs, ensuring that an attacker is presented with a blank screen rather than real data. These solutions do not rely on identification and eradication of malware but protect sensitive data regardless of the threats (known or unknown) present on the device.

Introducing more data threats and attacks

Other threats while data is in the application are DLL injection and MITB attacks. A DLL injection attack is a method of inserting malicious code into an application, providing access to sensitive data. MITB attacks generally use JavaScript code running in the browser, again providing dangerous access to malicious actors. Typically, an anti-virus solution is used to guard against malware attacks, but more effective are containerisation solutions and secure, locked-down browsers.

To tackle MITB attacks, the most effective method is a locked-down secure browser, which prevents any unauthorised java script code, or any browser extension to run in the browser preventing malicious activity. Containers are also a good prevention mechanism, allowing applications to be run inside a protected environment, ensuring only authorised code can run inside the environment, isolated from any malicious code which may be present on the device.

It is also very effective to run a secure locked-down browser within a container, add kernel-level keylogging protection and anti-screen capture methods, in order to provide a secure environment on an unmanaged, remote-access device such as a home PC or personal laptop.

And so on into the cloud

Many organisations now operate in the cloud and there is a risk while data is being transmitted from the endpoint to the cloud from man-in the-middle (MITM) attacks, such as files being uploaded, etc. Fortunately, due to the availability of effective solutions, these threats are relatively low, and encrypted mechanisms are effective. But once data reaches the cloud for processing or storage, it can become vulnerable to cloud-based attacks such as advanced persistent threats (APTs).

These are sophisticated attacks which continue over a long period, during which an attacker (once a foothold is gained) seeks to search and move around cloud storage, setting up data exfiltration or denial of service attacks. DDoS attacks are a common occurrence and frequently make headlines and defence techniques, including containerisation and DevOps, are well developed and well documented.

More people at home, more online

The risk of a breach is heightened not just because WFH is now so prevalent, but also due to a general rise in online activity by different people in the same household. Malicious actors are adept at identifying any vulnerability and the increase in usage of technology to access online games and stream videos is just as appealing to them as the number of employees using devices that are not fully managed. In fact, one of the areas in which we fully expect to see a jump in cyber activity is around children being targeted in order to get malicious code onto their parent's work devices. Once triggered, they will allow access to their company network.

Our advice is to encourage organisations to consider the broader picture when it comes to protecting their employees and their data. The risk profile of an individual needs to be extended to anyone they could potentially share their devices with, including family and friends. To keep individuals, the organisation and all connections safe, they need to look for solutions that are specifically designed to protect against all vulnerabilities, not just the most obvious ones.

References

1 National Cyber Security Centre (2020). *Annual Review 2020*. **http://bit.ly/NCSCAnnualReview20**

2 Interpol (2020). *Interpol report shows alarming rate of cyberattacks during COVID-19*. **http://bit.ly/InterpolReportCovid**

3 NTT Security (2019). *Global Threat Intelligence Report*. **http://bit.ly/NTTGlobalThreatReport**

About the author

Dave Waterson is CEO at SentryBay and an expert in endpoint and application security.

He was included amongst the top 10 tech thought leaders identified by A.T Kearney at the World Economic Forum in Davos and is a winner of the Great British Entrepreneur of the Year Award, for cyber security.