An analysis of the "Stolen Pencil" cyber-attack and other cyber-attacks against universities

u5539006 (Peter Walker)

February 2024

Contents

1 Executive Summary

Universities are prime targets for cyber-criminals due to owning a large amount of data, and managing a lot of finances. In this report, there is an analysis and explanation of the complex cyber-attack known as "Stolen Pencil", which affected educational institutions in 2018, a spear-phishing campaign which involved credential stealing and remotely connecting to compromised devices, and some recommendations for universities to reduce the likelihood of experiencing similar attacks, such as better training for all individuals, putting measures in place to analyse the systems, and blocking unnecessary services and protocols, using external devices.

2 Background

Universities are more likely than other educational institutions, and businesses, to experience cyber-attacks and breaches, in a wider range of forms (Official Statistics, 2023). As universities have access to highly sensitive and valuable data and a large attack surface (Luke Warren, 2023), they are a prime target for attackers, partly due to their common lack of security (Emma Woollacott, 2024).

Universities store unpublished research and intellectual property and keep extensive records of all students, including personal and financial information, and potentially medical records. All this data is valuable to attackers whether for financial gain or to tailor social engineering campaigns.

Between the large number of personal devices connected to university networks, the many networks (campus, departmental, personal), and network-enabled equipment, there are numerous entry points for attackers to gain unauthorised access. Furthermore, it is usually trivial to move through the university networks once access is gained due to poor personal cyber hygiene, and Single Sign-On (SSO) systems that many universities support across their resources (61% of higher educational institutions reported losing money or data or having compromised accounts used for illicit purposes following a breach, and 50% experience breaches or attacks at least weekly (Official Statistics, 2023)).

75% of universities in this study reported negative impacts regardless of material outcome, from both breaches and cyber-attacks.

2.1 Recent cyber-attacks against UK universities

Cyber-attacks on universities can disrupt services and resources, such as in the case when the Universities of Cambridge and Manchester were targeted with a DDoS (Distributed Denial-of-Service) attack in February 2024, which disrupted internet services and university resources by flooding them with arbitrary traffic so legitimate traffic is drowned out (Patrick Jack, 2024). The University of Wolverhampton also experienced a "systems issue" at the same time (Emma Woollacott, 2024). "Anonymous Sudan", who claimed the attack, cited political motivation for the attack, "because of the UK's continued support for Israel". These universities were targeted because "they are the biggest ones" they could find. These issues were resolved overnight, but lasted up to 24 hours, and access to university services was impossible from off-campus. The cost of the attack and the subsequent disruption is currently unknown.

There was another attack on the University of Manchester in June 2023, involving phishing emails to gain unauthorised access to, and steal, data as part of a ransomware attack. The attackers claimed they had stolen 7 terabytes of data (Sergiu Gatlan, 2023), but post-attack system analysis suggests only 250 gigabytes were accessed including up to 1.1 million NHS records (Rebecca Thomas, 2023), but apparently not including any financial information. The attackers threatened to sell the stolen data if "the university did not resolve the situation"

(BBC News, 2023), presumably by paying a ransom. Staff and students were advised to "carry on as usual", but recommended staff not to download files for backup purposes (Alex Scroxton, 2023). A few days later, password resets were required and off-campus access to university services was removed (Libby Elliott, 2023). The ICO has not released any information relating to potential fines or other consequences, though the university of Manchester has offered a year of Experian's IdentityWorks service, which monitors for theft, loss or disclosure of personal information on public services.

3 Analysis

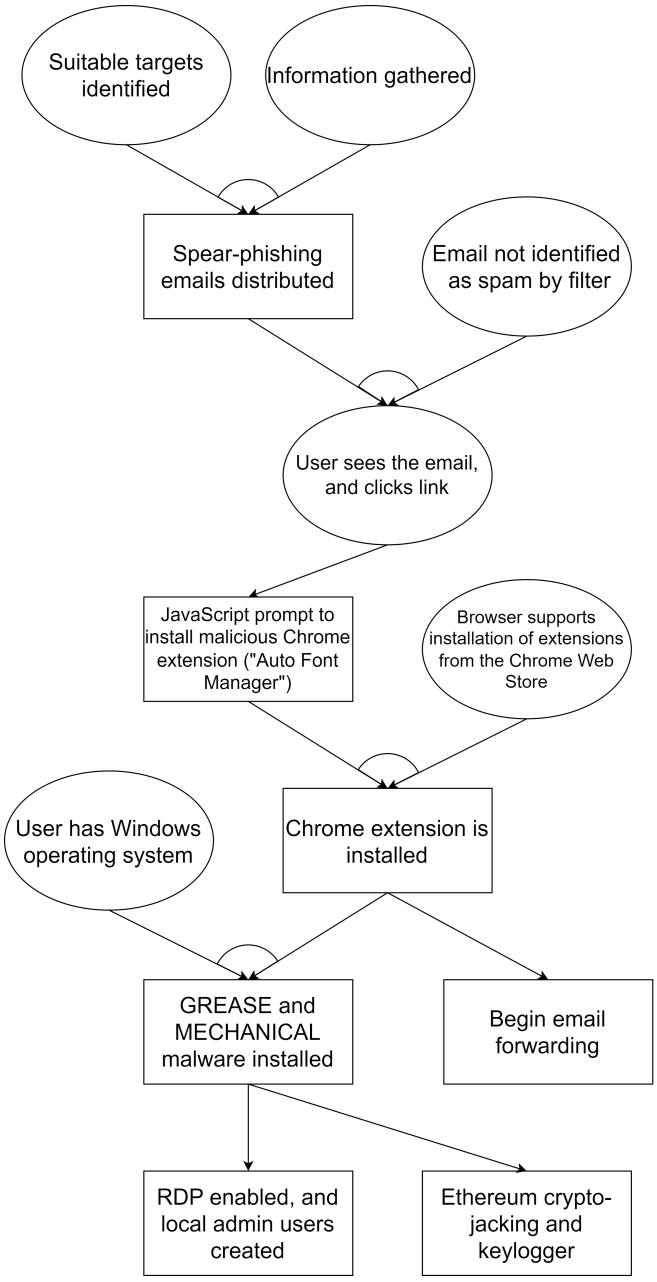

Figure 1: An attack graph demonstrating the “Stolen Pencil” cyber-attack

The section analyses the cyber-attack known at "Stolen Pencil", which involved credential harvesting targeting academics, generally attributed to the North Korean APT group "Kimsuky".

3.1 Weaponisation of information and Delivery

Academics were sent spear-phishing emails (emails that are targeting individuals or organisations personally, as this makes them appear legitimate (Bart Lenaerts-Bergmans, 2023)). The majority of these emails were sent to academics with "expertise in biomedical engineering" which may be a hint towards motivation for the attack, since the true motivation is not clear (ASERT Team, 2018). There was some variation in the type of phishing received: some redirected to fake login pages (that were just saved HTML pages from the Internet) for common websites, to harvest user credentials. The more complex scams displayed a harmless PDF file when the user clicked on a link. The PDF scams appeared to come from a post-secondary educational institution (Mount Royal University, 2018).

There is little evidence as to the nature of the emails, or from whom they came originally, however, email forwarding (of the spear-phishing emails) was observed on some compromised accounts. This is likely to contribute to email spam filter evasion, since the emails were coming from reputable domains of academic institutions (Sean Lyngaas, 2018).

The links that redirected to a harmless PDF, after a short delay, displayed a JavaScript alert (a small popup at the top of the window, stopping you interacting with your browser until you clear or accept it) informing them to "Please install new Font Manager to your Chrome!" (ASERT Team, 2018). Once this popup was interacted with, it would redirect the user to the Chrome Web Store, a website which allows the user to download 'extensions' to their browser, to "customize the browsing experience" (Chrome for Developers, 2013).

3.2 Exploitation

On the Chrome Web Store page, there was an extension called "Auto Font Manager" (see Figure 2) which, once installed, had permission to be active on all URLs (so all websites visited), see active tabs, look at cookies (which can give away personal information), and store any information it finds persistently, even if the users cleared cookies, browsing history, cache etc. This means it could send data about the user, their activity, and any data other websites may store about them, to the attacker.

The code for this extension could not be analysed, as the attackers replaced the malicious JavaScript file (retrieved from an external server), with a benign one when the attack was discovered. It is almost certain that this was the location of the malicious code, as the original file of the same name ("jQuery.js" -

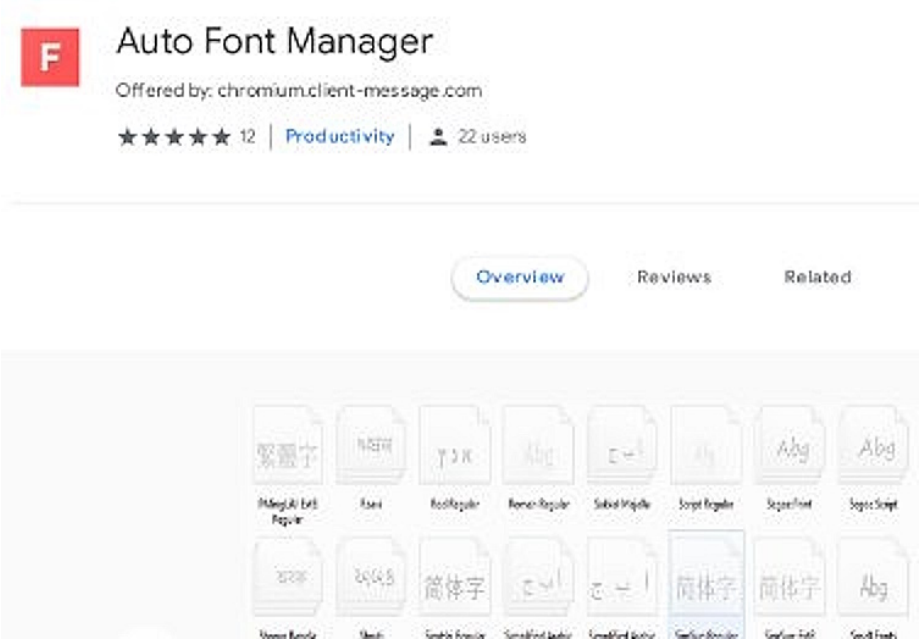

Figure 2: A screenshot of the "Auto Font Manager" in the Chrome Web Store

a standard JavaScript source library) was bundled in the extension in its original state, so it doesn't make sense to load it from an external source (ASERT Team, 2018).

The extension was made to seem more legitimate by giving it 5-star reviews from previously compromised Google accounts. The text for each review was copied from other chrome extensions, but was a mix of positive and negative feedback, despite being given the highest rating every time (ASERT Team, 2018).

It is unclear how the attackers went from control over the browser to being able to run software on the victim's machine, and it is even possible that it may be a separate attack. However, NETSCOUT, who discovered and documented the attack, believe it to be related due to the attacks utilising the same infrastructure and targeting the same people (Catalin Cimpanu, 2018).

3.3 Installation

By using portable executables, software designed to run on any platform of the Windows operating system, the attackers executed the homemade (Scott Ferguson, 2018) GREASE and MECHANICAL malware on the compromised machines.

The attackers used the GREASE malware (CISA, 2020) to achieve "point-and-click" access (interacting with a computer as though you are sat in front of its keyboard and mouse) on the compromised machines, which involves using Microsoft's Remote Desktop Protocol (RDP) to control the machines over the Internet (remote access). They also used GREASE to add a local administrator account to the system and enabled RDP. The attackers created the local admin account with common usernames such as "LocalAdmin"" and "DefaultAccounts" to reduce likelihood of detection (ASERT Team, 2018). RDP could be enabled on these compromised machines despite any firewall rules (such as Windows Firewall's default settings)

The other malware ran on the machines was MECHANICAL. This is a keylogger and crypto-jacker, meaning it would record all inputs to the machine from keyboards including passwords and financial information entered, and presumably send it back to the attackers. It would also replace any 'Ethereum' (a cryptocurrency) addresses with the attacker's own wallet address. This would mean any 'Ethereum' transferred by the users would be rerouted to the attacker's address.

3.4 Command and Control

The attackers regularly connected to the compromised devices through RDP in the early hours of the morning through a command-and-control server (a proxy server, which makes tracking the person connected harder by routing the connection through another device), but it did not appear as though any data was stolen from the machines themselves. The only harvested data seems to be credentials. After further analysis, the only tools found on compromised machines seemed to be for reconnaissance (understanding and learning about systems and accounts) and further password theft (ASERT Team, 2018), as well as some for compromising other connected devices (HYPR, n.d.).

3.5 Actions and Impact

As the attackers put measures in place to achieve persistent access (RDP), they could still access the PC even if the initial intrusion vector was closed, so it seems likely that the attack was interrupted before they could steal the data they wanted, or disrupt any systems, since no such thing happened. It is undisclosed which institutions were affected by this attack, and so is it difficult to estimate the impact of this attack, beyond having credentials stolen.

4 Recommendations

These are the top five steps that the university can take to decrease the likelihood of the University of Barwick experiencing a similar cyber-attack:

4.1 Cyber Security Awareness Training

It is important for all individuals with access to university systems or networks to have at least basic cyber security awareness training. This would involve being taught about phishing emails, and the importance of password hygiene. This would help to minimise the impact of any cyber-attack as it is likely less individuals would fall for a scam nad therefore less devices would be compromised, and if any did, any credentials harvested would (hopefully!) be unique and would not be reused for any other systems or accounts, limiting their use to the attackers.

4.2 Reduce Attack Surface

Minimising the number of entry points for potential attackers to gain access to systems or networks is also very important. This is achieved by using the "least-privilege" principle (do not give any users more access or privileges than they absolutely require to perform the tasks they need to do) for users, removing user accounts that are no longer in use to reduce the number of potential targets, removing any software that is no longer required in case it develops a vulnerability, and reducing the number of linked services for students and staff to the bare minimum. This means that there are less targets for the attackers, which makes it more difficult for them to find an easy attack vector to begin an attack.

4.3 Regular Systems Audit

This involves regularly (at least monthly, if not more often) doing a full system audit of software, files, users, logs and devices. This allows the university to identify strange processes and pieces of software that would be unexpected, if any supposedly inactive users had been active, any log files for suspicious connections or processes, and check the connected devices are standard. It would involve someone, or a small team, (perhaps with software aid) going through absolutely everything on the university system and checking to see if anything looked out of place. This would allow any malware or suspicious files to be identified early, hopefully before they cause any damage.

4.4 External Security Devices

It would be a good idea to block unneeded services and protocols on the networks and devices by having security devices between the networks and the Internet, such as a firewall. This would allow for blocking of RDP that would be much

more difficult to circumvent, and any other services that are unneeded could be blocked as well. It would be worth considering implementing a "Zone-based Policy Firewall" to allow access to certain services from off-campus via the Internet, but keeping access to university devices, and services that wouldn't be needed off-campus restricted to users connected to the campus network. This would mean it was much more difficult to access critical services and devices from off-campus, limiting the effect any external attackers could have.

4.5 Funded Antivirus Software

The final recommendation is for the university to fund anti-virus software for students and staff personal devices. This would also be installed on all university machines, but individuals would be more inclined to use it if it was free and they did not have to pay for it themselves. This would help to secure the university networks since these devices would be connected, and could spread viruses and other malware across the network from personal devices if it was not identified. This would help to reduce the spread of malware across the university network, since it is more likely that the malware will be identified on the host device (because of the free antivirus) and isolated or removed.

References

[1] Official Statistics. *Cyber security breaches survey 2023: education institutions annex*. 2023. URL: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023-education-institutions-annex.

[2] Luke Warren. *Why are universities so attractive to cyber criminals?* 2023. URL: https://www.linkedin.com/pulse/why-universities-so-attractive-cyber-criminals-luke-warren/.

[3] Emma Woollacott. *UK universities left scrambling in wake of cyber attacks*. 2024. URL: https://www.itpro.com/security/uk-universities-left-scrambling-in-wake-of-cyber-attacks.

[4] Patrick Jack. *UK universities targeted by cyberattack*. 2024. URL: https://www.timeshighereducation.com/news/uk-universities-targeted-cyber-attack.

[5] Sergiu Gatlan. *University of Manchester confirms data theft in recent cyberattack*. 2023. URL: https://www.bleepingcomputer.com/news/security/university-of-manchester-confirms-data-theft-in-recent-cyberattack/.

[6] Rebecca Thomas. *More than a million NHS patients' details compromised after cyberattack*. 2023. URL: https://www.independent.co.uk/news/health/nhs-patient-data-attack-b2364202.html.

[7] BBC News. *University of Manchester: Students and staff sent data leak threat*. 2023. URL: https://www.bbc.co.uk/news/uk-england-manchester-65973785.

[8] Alex Scroxton. *University of Manchester hit by cyber attack*. 2023. URL: https://www.computerweekly.com/news/366539712/University-of-Manchester-hit-by-cyber-attack.

[9] Libby Elliott. *UoM students threatened with "data leakage" following cyber attack*. 2023. URL: https://mancunion.com/2023/06/21/uom-students-threatened-with-data-leakage-following-cyber-attack/.

[10] Bart Lenaerts-Bergmans. *WHAT IS SPEAR-PHISHING? — DEFINITION WITH EXAMPLES*. 2023. URL: https://www.crowdstrike.com/cybersecurity-101/phishing/spear-phishing/.

[11] ASERT Team. *STOLEN PENCIL Campaign Targets Academia*. 2018. URL: https://www.netscout.com/blog/asert/stolen-pencil-campaign-targets-academia.

[12] Mount Royal University. *Academic institutions targeted with malicious Chrome extension*. 2018. URL: https://blogs.mtroyal.ca/itsecurityawareness/2018/12/06/academic-institutions-targeted-with-malicious-chrome-extension-12-06-18/.

[13] Sean Lyngaas. *Suspected North Korean hackers target universities using Chrome extension*. 2018. URL: https://cyberscoop.com/suspected-north-korean-hackers-target-universities-using-chrome-extension/.

[14] Chrome for Developers. *What are extensions?* 2013. URL: https://developer.chrome.com/docs/extensions/mv2/overview.

[15] Catalin Cimpanu. *Cyber-espionage group uses Chrome extension to infect victims*. 2018. URL: https://www.zdnet.com/article/cyber-espionage-group-uses-chrome-extension-to-infect-victims/.

[16] Scott Ferguson. *North Korean-Backed Group Suspected of 'Stolen Pencil' Campaign*. 2018. URL: https://www.darkreading.com/endpoint-security/north-korean-backed-group-suspected-of-stolen-pencil-campaign.

[17] CISA. "North Korean Advanced Persistent Threat — Focus: Kimsuky". In: (2020). URL: https://www.cisa.gov/sites/default/files/publications/TLP-WHITE_AA20-301A_North_Korean_APT_Focus_Kimsuky.pdf.

[18] HYPR. *What is EternalBlue?* URL: https://www.hypr.com/security-encyclopedia/eternalblue.