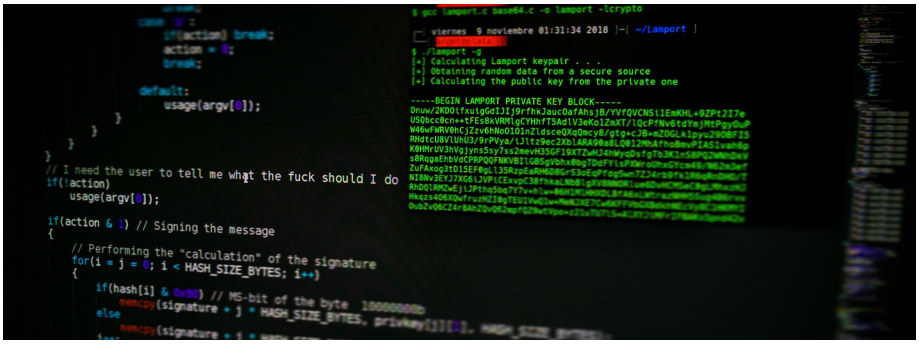
A Trend Micro White Paper | **June 2020**

Protecting UK Universities in the Covid 19 era

Introduction

Universities play a key role in the economy by innovating and providing skills to the next generation of industry talent across the globe. But this certainly poses a problem as a vast amount of intellectual property, personal and research data is created and handled, each with its own value on the dark web or to others in general.

With new student numbers expected to be significantly reduced come the new Academic year due to the global Covid-19 pandemic, Universities will inevitably suffer with a decrease in revenue for 2020-21 - https://www.timeshighereducation.com/news/uk-universities-face-ps26bn-coronavirus-hit-30k-jobs-risk - As such, this makes the research data that Universities hold even more valuable for the institution.



Cybercrime is a threat to all businesses as cyber criminals seek to make money through the sale or ransom of stolen data and information, Universities are seeing an increased number of attacks a cross a number of attack vectors. In addition to the breaches that we see in the news, Universities that Trend Micro speak to, are also experiencing a much larger problem of nation state attacks.

Where there are opportunities, there are perpetrators who attack, steal, and abuse the system for a wide variety of reasons. These threat actors can be criminal gangs that are highly skilled hacking teams, funded and controlled by organized criminal gangs or sometimes even governments, and they target victims using different methods such as ransomware, phishing and so on to generate illicit revenue for malicious actions for political reasons.

State sponsored attacks are almost certainly targeting Universities for the research data and information they hold which would otherwise be unavailable to them. Many Universities have partnerships with global corporations supplying research data that ranges from a medical, defence and commercial sensitivity. Any loss of this data would almost certainly be detrimental to the University and even the UK as a whole, often the Universities reputation is what attracts top professors and academics, which in turn attracts global students.

Research data holds a lot of value and we have seen and heard of numerous types of attacks being used. Attackers are innovating and coming up with new ways to try and gain an advantage as well as using tried and tested techniques of social engineering, credential phishing and account compromise. In extreme cases nation states have sponsored attacks which have involved enrolling students onto courses with the intention of identifying and exfiltrating valuable data covertly. It's not just data and information though that criminals are trying to gain, some of these attacks have the primary goal of duping staff into making performing a task that involves transferring something that has a monetary value.

How are Universities successfully attacked?

The very nature of Universities and how they operate means that they are open and welcoming, networks are diverse and sometimes the lines between student and staff access can get blurred.

The requirement for academics to use their own laptops and research equipment along with students requiring access to multiple cloud services and providers means that there is a raft of shadow IT going on.

Often Universities are impacted by untargeted attacks, back in June 2018 a widely distributed ransomware attack had a significant impact to multiple Universities, with systems and information locked until the ransom was paid.

Whilst rare, targeted attacks do occur and have potential to have larger financial impact. The use of compromised accounts could lead to payments being made to unintended recipients or even spoofed email accounts that impersonate a staff member (Business Email Compromise), supplier or University partner. Both of which have led to sensitive information or funds being supplied to criminals.

Attack Vectors and Challenges

When we speak to our University customers, we are often told about the constant struggle to combat phishing attacks. Information is key to a successful phishing attack and social engineering is often easy to perform. University websites and social media sites provide a wealth of information and with a cleverly crafted message it can be easy to trick a student or staff member into performing actions that leads to a breach. Multiple times people have supplied logon credentials or spread malware unwittingly and the worst-case scenario even made payments to a fraudulent recipient.

During the Covid-19 lockdown period, we have seen our University customers being targeted with attacks using Emotet and Psuedoderm techniques trying to enter the University via email. Also, during the lockdown period, many Universities have accelerated their use of Amazon Web Services (AWS) and Microsoft Azure. This again has opened a new attack vector and added more security challenges for the Infosec Teams.

Education of staff and students plays a huge part in providing a defence against the kind of attacks, so running training programs to help staff should be key. The problem is that sometimes people think they are being unfairly singled out, but we should all realise that this kind of training helps in our own lives as well and is something we can make our own siblings aware of. Training however doesn't mean that we should not have strong perimeter defences, a solution that can identify malware, phishing attacks and business email compromise is a must.

Network Design

Another challenge for Universities is the network design, how can we ensure the network is sufficiently protected and also a constant stable platform for information to be accessed and shared across the faculties.

Many Universities have a number of faculties that require their own private network or require less restrictive security controls due to the research they are carrying out. These smaller pockets of networks are likely to be more vulnerable and may not be managed by a trained network specialist, often its difficult to change the "This is how its always been" mentality to apply greater vulnerability protection and monitoring. Research into medical devices and IOT devices may also mean that it's not possible to apply protection to the endpoint/devices themselves, so how do we ensure that there is sufficient protection in these areas as well.

What Next?

As we innovate and adopt new technologies, particularly in the cloud, the attack surface is going to increase while threats are constantly evolving and becoming increasingly sophisticated. Staff are having to be more vigilant and IT staff more aware of the vulnerabilities that exist in the network and this isn't going to change.

Being able to identify what happened when and to who is a basic requirement but often a daunting process. Security engineers and the Security Operations Centres (SOC) are often overwhelmed by alerts and knowing where to focus their attention when a breach occurs, having siloed security solutions feeding into a SIEM or just having to piece together the individual logs can be overwhelming and time consuming, often when something is detected it's too late. Reducing alert fatigue and being able to reduce investigation time for any breach is key to understanding where to focus resource, whether that be financial or additional training for staff.

Conclusion

While Universities continue to carry out high value research and generate information that is of interest, they will almost certainly be a target from hacktervists, nation states and cyber criminals. If successful the impact of a breach could cause more damage reputationally or through fines than the cost of the data itself.

How Can Trend Micro Help?

Email & File Collaboration Services Protection

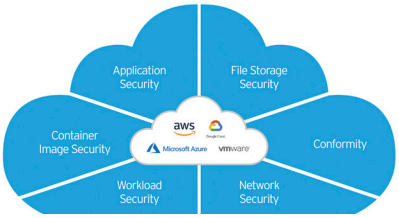
Cloud App Security integrates directly with Office 365, Gmail and other services using application programming interfaces (APIs), maintaining all user functionality without rerouting email traffic or setting up a web proxy.

Key Benefits

- ✓ Protects Office365 and Gmail email, along with other cloud file-sharing and collaboration services, including Teams, which has seen a huge uptake in usage during the Covid-19 lockdown.
- ✓ Detects ransomware and other malware hidden in Office file formats or PDF documents
- ✓ Identifies BEC attacks using artificial intelligence
- ✓ Protects internal email and allows on-demand scanning for mail store
- ✓ Gives visibility into sensitive data use with cloud file-sharing services
- ✓ Preserves all user functionality, on any device, with simple API integration

Cloud Protection and Compliance

Trend Micro Cloud One is a cloud-native security delivers new functionalities with no impact on access or experience. It seamlessly complements and integrates with existing AWS, Microsoft Azure, VMware and Google Cloud toolsets.



Part of Cloud One is Cloud Conformity and businesses use Cloud Conformity to monitor their security and compliance best practices in the cloud. This is particularly useful for Universities who are just starting on their journey in their cloud. It gives them real-time visibility across all cloud accounts in one place and the actionable remediation guidance delivered through chosen integrations. This shrinks the time to identify and remediate security threats or misconfigurations in the cloud.

It also changes the way developers build and operate in the cloud resulting in software being built better, and faster. It ultimately provides businesses confidence that as they scale in the cloud, they are doing it in a compliant fashion.

Powerful network layer security for the hybrid cloud without disruption

You need counter measures to ensure that malicious activity moving across your network from infected machines is detected and dealt with appropriately. Trend Micro Deep Discovery and TippingPoint solutions will work together to detect and prevent lateral movement. With the ability to deploy in the cloud network fabric, and quickly gain broad protection and compliance, Trend Micro Cloud One Network Security is the network security solution you need to achieve your multi-layered security strategy. Network Security automates actionable security for virtual private clouds (VPCs) and cloud networks by simplifying network security in the cloud, while maintaining the ability to inspect ingress and egress traffic. Using an agile, inline deployment approach and flexible failover scenarios, it ensures enterprises can protect their cloud networks without disrupting their applications. Network Security provides industry-leading coverage across multiple threat vectors, offering comprehensive threat protection that includes virtual patching, vulnerability shielding, exploit blocking, and high-accuracy defense against known and zero-day attacks.

Network inspection provides a 360 degree view of your network to create complete visibility into all aspects of targeted attacks, advanced threats and ransomware. By using specialised detection engines and custom sandbox analysis, Deep Discovery Inspector identifies advanced and unknown malware, ransomware, zero-day exploits, command and control C&C communications, and evasive attacker activities that are invisible to standard security defences. Detection is enhanced by monitoring all physical, virtual, north-south and east-west traffic.

TREND MICRO™
Securing Your Connected World

Trend Micro Incorporated is a pioneer in secure content and threat management. Founded in 1988, Trend Micro provides individuals and organizations of all sizes with award-winning security software, hardware and services. With headquarters in Tokyo and operations in more than 30 countries, Trend Micro solutions are sold through corporate and value-added resellers and service providers worldwide. For additional information and evaluation copies of Trend Micro products and services, visit our Web site at www.trendmicro.com.

TREND MICRO INC.
Eric Graves
Account Director – UK Education
eric_graves@trendmicro.com
+ 44 (0) 758 179 5045