BURK I.T.

1440 E Shipley Ferry Road
Kingsport, TN 37663

Get the Digital Version!

Check Out the Website!

Follow Our Social Media!

Inside This Issue

- News.exe | Virtual Reality
- Burk Blog | MFA in the USA
- Product Feature | SentinelOne
- Client Spotlight | Associated Oral & Implant Surgeons
- What's New | Bram Sword

Virtual Reality | News.exe

You have likely heard of virtual reality, or VR for short. In this case, I am referring primarily to true, total VR, as I think augmented reality is worthy of its own explanation at some other time. The term "virtual reality" has only existed in its current understanding since the 80s, when Jaron Lanier designed some of the first high-end virtual reality hardware under his firm VPL Research. VR, in more a theoretical sense, has been popularized by films like Lawnmower Man and Tron. Only very recently has VR technology become practically available to the average consumer, though even now, it's still a relatively niche market.

The 1990s saw the first widespread commercial releases of consumer headsets. In 1992, for instance, Computer Gaming World predicted quote "affordable VR by 1994". However, this was a woeful misunderstanding of the technology and its applications at that time. In the early days of VR, it was prohibitively expensive for any normal consumer to acquire any of these products. In addition, the graphical capabilities of the early VR headsets were extremely limited by technology at that time. With headsets that put screens literal inches away from the users' eyes, no software developed for early VR could be anywhere near realistic, even for graphical standards at the time. VR required some of the world's best computers to run at all in the 90s, meaning that VR was relegated largely to gimmick arcade machines and some technical, practical applications.

The pioneers of VR in the late 80s and early 90s needed a way to secure funding for research and development of these first VR systems, and much of that funding was justified by the practical applications for VR, which are still used today. VR allows for training in...

NEWS.exe

WATCH THE SHOW

THE BURK Bulletin

Product Spotlight | SentinelOne

SentinelOne is an advanced EDR and threat hunting solution that delivers real-time visibility with contextualized, correlated insights accelerating triaging and root cause analysis. The solution lightens the SOC burden with automated threat resolution, dramatically reducing the mean time to remediate (MTTR) the incident. ActiveEDR enables proactive hunting capabilities to uncover stealthy, sophisticated threats lurking in the environment.

Burk IT has deployed SentinelOne Next Generation Endpoint Security & Advanced Malware Protection agents on all workstations and servers we support. This solution provides holistic protection against all forms of malware and malicious exploits including executables, fileless memory attacks, document infections, browser exploits, malicious scripts, and credential-based attacks. SentinelOne is A.I.-based, monitoring user, network, application, and operating system behavior to detect and remediate threats. As such, it is not signature file dependent. This product is monitored in real-time by a 24/7/365 security operations center staffed with security analysts who in turn report all issues immediately via email and phone to Burk IT. Remediation is also performed in real-time.

With intelligent automation becoming an obvious replacement for signature-based detection, SentinelOne offers a comprehensive solution for servers and endpoints. SentinelOne offers a lightweight solution secures endpoints and servers without compromising performance. Behavioral threat analysis that leverages machine learning to capture and neutralize both known and unknown threats, while providing a forensics package that allows administrators to visualize attack paths and remediate vulnerabilities quickly and efficiently.

In terms of mitigation, SentinelOne can block and identify malware, even if it hasn't been seen before in the wild. In Alert Mode, it can identify malware, such as ransomware, and detect malicious behavior, such as creating an executable file without permission. SentinelOne will display the entire attack path of malware— and then enable administrators to seamlessly rollback an infected machine.

With SentinelOne, IT teams finally have a viable path forward that allows them to stay ahead in the arms race against bad actors. Instead of spending limited time, money, and manpower remediating breaches that are already in progress, security practitioners can now usefully devote their time to reinforcing the solid foundation which SentinelOne provides.

Client Spotlight

Burk IT is exactly what we hoped for when we decided to search for an IT partner who understands the complexity of our business and can meet our needs with outstanding customer service. We have absolute confidence that our hardware/software is protected, within compliance, and optimized to our specific needs. What separates Burk IT from the rest is their responsiveness to any issues that impact our operations. It's great to have the right IT protection, but it's a truly valuable partnership when they respond as quickly as they do in such a professional manner. They collaborate with us on every IT need, whether small or large and always explain things clearly and concisely. Their (Quarterly Business Review) QBR is insightful and reinforces their commitment to be a partner and not just a service provider.

Daniel M. Tackling
Director of Operations
Associated Oral & Implant Surgeons

MANAGED SERVICES • 423.578.8000 • WWW.BURKITC.COM
BURK I.T.

What's New

Bram Sword is a systems engineer at Burk I.T. He has been working in the IT field for over 6 years, having worked in retail computer support to managed service providers, doing everything from basic desktop support high-end server maintenance. As an IT professional, he believes in going above and beyond in every situation, whether implementing new software or supporting what is already installed. He always strives to give the best client experience possible. In his free time, he is a musician, playing guitar, bass, and drums.

August 2022

This monthly publication provided courtesy of Stephenie Griffith and the Sales & Marketing Team at Burk I.T.

Our Mission

To create trusted relationships while providing Practical, Secure IT Results
That's the Burk I.T. Way

Does the Vendor Matter?

Recently I was asked to discuss the cybersecurity risks associated with smartphones and the possibility that those devices could be compromised and information stolen. As part of the conversation, an all too familiar story was told about an older gentleman who had been prompted through a fear-based social engineering phone call to go to the bank and withdraw a significant amount of money to avoid some fictitious financial penalty.
What was a little more unique in this situation was the fact that the older gentlemen had also been prompted to download an app on his smartphone that had in turn given the attacker control of that device. Fortunately, an alert bank employee noticed something strange during the transaction as the older gentleman continued to receive directions from the attacker via his phone. The bank employee intervened and, after some effort, was able to power off the gentleman's phone and get to the bottom of the scam.

Sadly, this is not a terribly unique situation. Creative and malicious vishing (voice phishing) attacks take place everyday, targeting young and old alike. What is a little more concerning is the evolution of malicious applications and the use of these applications to take remote control of a device during a social engineering attack, thus giving the attacker near complete control over the situation and ramping up the fear factor for the victim.

In the situation with the older gentleman at the bank, his problems did not end once the attack was discovered and his phone was powered off. At that point, his smartphone, a low cost, prepaid Android device, was compromised and unsafe to use. The bank employee rightly recommended he factory reset the device or replace it, but neither option was honestly viable for the victim. He lacked the technical skill to properly reset the device and he could not afford to simply throw it away and buy another one. Because it was a big box store...