



Monthly InfoSec Newsletter April 2021



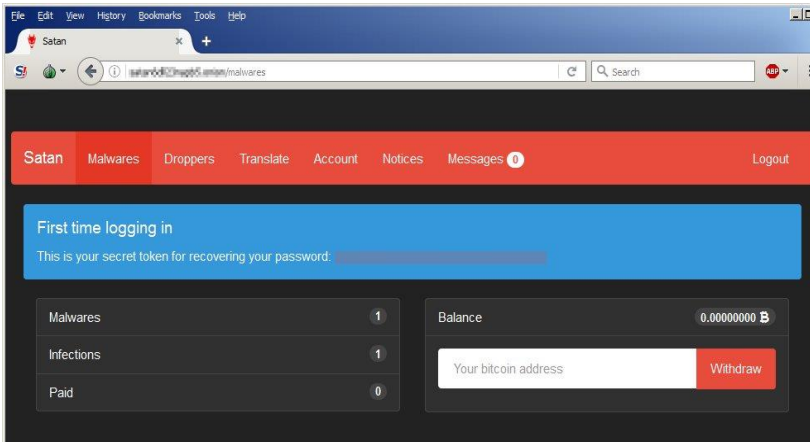
IRS warns university students and staff of impersonation email scam

The Internal Revenue Service today warned of an ongoing IRS-impersonation scam that appears to primarily target **educational institutions**. The IRS' has received complaints about the impersonation scam in recent weeks from people with email addresses ending in ".edu."

The suspect emails display the IRS logo and use various subject lines such as "Tax Refund Payment" or "Recalculation of your tax refund payment." It asks people to click a link and submit a form to claim their refund.

You can read the full article here

<https://www.irs.gov/newsroom/irs-warns-university-students-and-staff-of-impersonation-email-scam>



Ransomware as a Service or RaaS

Ransomware is a form of malware that seeks to stop the user from accessing their files by encrypting them. The attacker requires payment (i.e. a ransom) before allowing the legitimate user access to their files. If the ransom is not paid, the legitimate user does not receive the key to unencrypt their files and in some cases, the legitimate user's files are broadcasted over the Internet for all the world to see. These attacks have been around for decades, but more recently vendors on the dark web are offering tools to order attacks easily and discretely. The developer will create a generic form of Ransomware and sell it on the dark web to people who want to do harm.

A purchaser of ransomware can now contract with bad actors to share the profits of the ransom, thus developing Ransomware-as-a-Service (RaaS). Today, RaaS contracts could earn the purchaser up to 70% of the profits. There are an estimated 25 large scale providers of RaaS over the dark web that distribute these extremely dangerous services to many people and causing a large security risk. The image above is the website of a bad actor who offers RaaS.

PCI DSS Annual Audit and Compliance

Payment Card Industry (PCI) compliance is a set of standards that governs credit card processing security for any institution or business that runs transactions through the 4 major credit cards brands (Visa, MasterCard, Discover, and American Express). PCI compliance ensures that businesses are doing their due diligence to protect cardholder or customer data and reduce credit card fraud.

Our CSU Pueblo Information Technology (IT) and Business Financial Services (BFS) together, are conducting our annual PCI audits and training for each department on our campus that handles credit card data. This is done to ensure that we are compliant with PCI regulations and also so ensure that we are safely handling credit card data of our campus family.

CSU Pueblo

Information Security Webpage: <https://www.csupueblo.edu/information-technology/security/index.html>

- Previous Monthly Newsletters
- Information Security (InfoSec) Monthly Newsletters
- InfoSec Awareness