Security researcher pleads guilty to hacking into Microsoft and Nintendo

A 24-year-old security researcher narrowly avoided prison today, after admitting to hacking into Microsoft and Nintendo servers and stealing confidential information. Zammis Clark, known online as Slipstream or Raylee, was charged on multiple counts of computer misuse offenses in a London Crown Court on Thursday, and pleaded guilty to hacking into Microsoft and Nintendo networks.

Prosecutors revealed that Clark had gained access to a Microsoft server on January 24th, 2017 using an internal username and password, and then uploaded a web shell to remotely access Microsoft's network freely for at least three weeks. Clark then uploaded multiple shells which allowed him to search through Microsoft's network, upload files, and download data.

In total, around 43,000 files were stolen after Clark targeted Microsoft's internal Windows flighting servers. These servers contain confidential copies of pre-release versions of Windows, and are used to distribute early beta code to developers working on Windows. Clark targeted unique build numbers to gain information on pre-release versions of Windows in around 7,500 searches for unreleased products, codenames, and build numbers.

IRC and web shells were key parts of the intrusions

Clark then shared access to Microsoft's servers through an Internet Relay Chat (IRC) server chatroom, allowing other individuals to access and steal confidential information.

Prosecutors say other hackers from France, Germany, the United Arab Emirates, and other countries were then able to access Microsoft's servers. Police found the stolen files on Clark's home computer after a joint investigation involving Microsoft's cyber team, the FBI, EUROPOL, and the NCA's National Cyber Crime Unit (NCCU).

26-year-old Thomas Hounsell, known in the Windows community for running the now discontinued BuildFeed website, also appeared alongside Clark in court on Thursday. Hounsell has always closely followed Microsoft's development processes and used Clark's server breach to conduct more than 1,000 searches for products, codenames, and build numbers over a 17-day period.

Photo by James Bareham / The Verge

Nintendo estimated damages of up to $1.8 million

The Microsoft intrusion ended when Clark uploaded malware onto Microsoft's network, and he was subsequently arrested in June, 2017. Clark was then bailed without any restrictions on his computer use, and went on to hack into Nintendo's internal network in March last year. Clark gained access through Virtual Private Networks (VPNs) and used similar software to hack into Nintendo's highly confidential game development servers. These servers store development code for unreleased games, and Clark was able to steal 2,365 usernames and passwords until Nintendo eventually discovered the breach in May 2018. Nintendo estimates the cost of damages between £700,000 ($913,000) and £1.4 million ($1.8 million), and Microsoft previously provided the court with a vague estimate of around $2 million in damages.

Clark, who was employed at the Malwarebytes security company at the time of the Microsoft hack, was also previously cautioned by British police after being arrested for his role in the massive Vtech data breach in 2015. Clark accessed the

account details of millions of Vtech toy users, including children's accounts. Names, dates of birth, profile images, and even addresses were stolen. Clark fully admitted to the Vtech breach, but the toymaker did not wish to assist with the prosecution so the case went no further. Vtech was eventually fined $650,000 for violating children's privacy. Clark has also been involved in security research for a number of years, previously uncovering flaws in school internet monitoring software and preinstalled apps on laptops sold by Dell, Lenovo, and Toshiba.

The judge commended Clark's parents

Clark's defense barrister said that because the former security researcher is an autistic person and has face blindness, he would be highly vulnerable to violence from fellow prisoners or even at a greater risk of reoffending if imprisoned for his crimes. Sentencing Clark, Judge Alexander Milne, QC, compared the offenses to that of a common burglar who had entered a house, stolen goods, and altered a home. While the offenses are certainly serious, and similar cases have involved jail sentences, the judge weighed up the unique aspects of this particular case. "Everything I have heard and been told leads me to believe this is a young man who would suffer disproportionality if he went to prison," said Judge Milne. The judge revealed a letter penned by Clark's parents, detailing his plans for rehabilitation and his challenges with autism, had weighed heavily on his decision. Clark's mother has given up her day job to help supervise her son and work on his rehabilitation, and the case had clearly taken its toll on the family. "The heartbreak, and I can only see it as heartbreak for his parents, comes across loud and clear. They are to be commended," said Judge Milne.

Clark was sentenced to a total of 15 months imprisonment, suspended for 18 months. A Serious Crime Prevention Order was also granted for a period of five years, which carries an unlimited fine and up to five years in prison if breached.

Hounsell was also sentenced to six months imprisonment, suspended for 18 months, and given 100 hours of community service.

These suspended sentences mean neither Clark or Hounsell will spend immediate time in prison, providing they don't reoffend. Ending his sentencing, Judge Milne said "I am trusting this will be a lesson from which you will all learn."

"Today's action by the Courts in the UK represents an important step. Stronger internet security not only requires strong technical capability but the willingness to acknowledge issues publicly and refer them to law enforcement. No company is immune from cybercrime. No customer data was accessed, and we're confident in the integrity of our software and systems. We have comprehensive measures in place to prevent, detect, and respond to attacks," says Tom Burt, CVP of customer security and trust at Microsoft in a statement to *The Verge*.

We've also reached out to Nintendo for comment on the sentences, but the company did not respond in time for publication.

https://www.theverge.com/2019/3/28/18286027/microsoft-nintendo-vtech-security-hack-breach-researcher-guilty