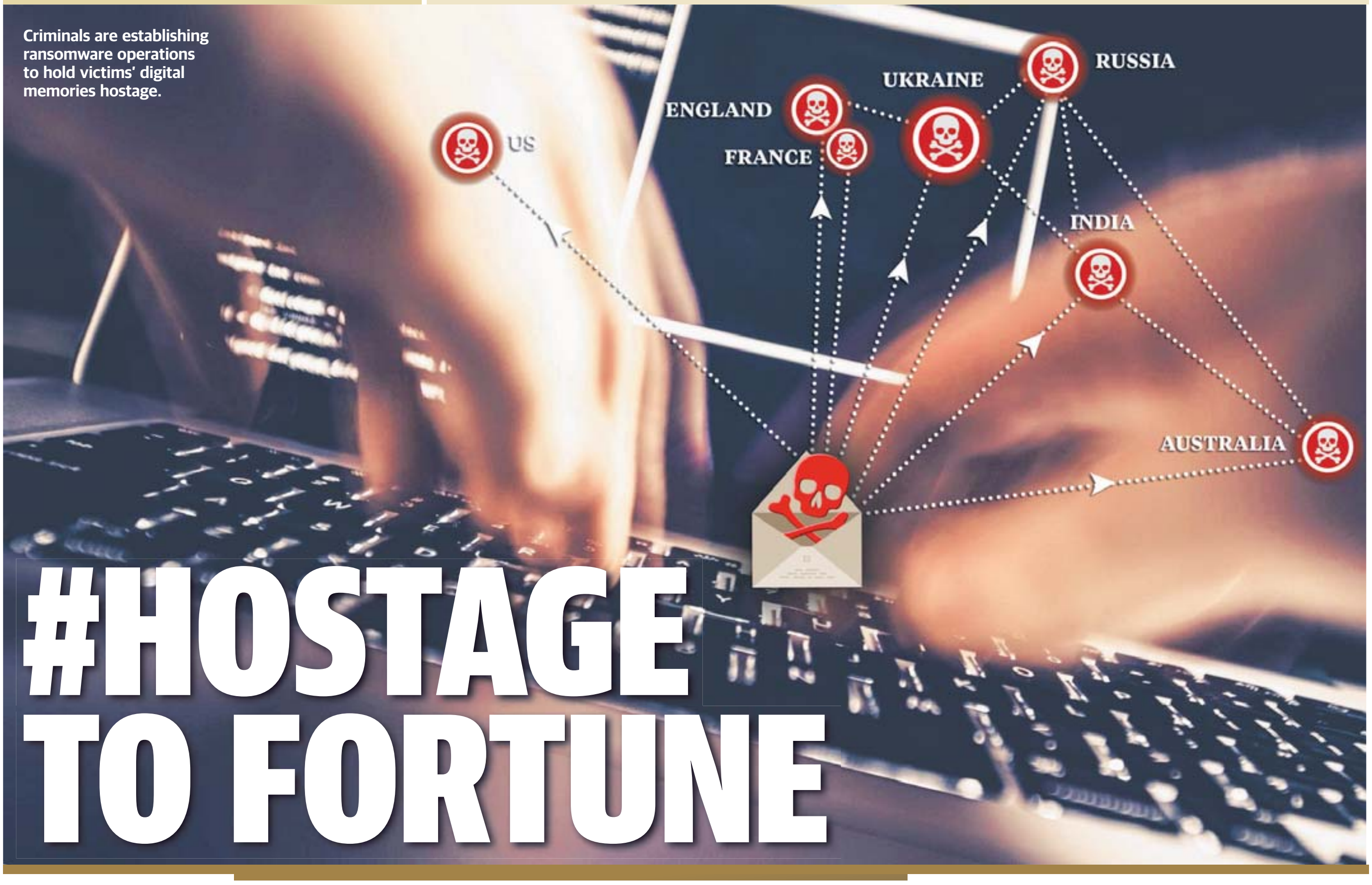
01 Jul 2017
Daily Telegraph, Sydney

Author: Jennifer Dudley-nicholson • Section: General News • Article type : News Item
Audience : 235,091 • Page: 64 • Printed Size: 1060.00cm² • Market: NSW
Country: Australia • Words: 1083 • Item ID: 802540786

isentia.mediaportal



Criminals are establishing ransomware operations to hold victims' digital memories hostage.

#HOSTAGE TO FORTUNE

AUSTRALIA IS BEING TARGETED BY CYBER CRIMINALS WHO WILL STOP AT NOTHING, WRITES **JENNIFER DUDLEY-NICHOLSON**

Australia's remote location offers no protection from the new wave of cyber-blackmail that rates us a prime target for ruthless hackers.

There was once a code of conduct that decreed no hacker should target critical infrastructure or endanger lives. But this week's global attack on power grids, banks, an airport, a pharmaceutical firm and part of the Chernobyl nuclear facility showed no mercy. And Australian firms were caught in the chaos, with work stalled at Cadbury factories, TNT Express, law firms and an advertising company.

Security experts warn it's an insidious escalation of a popular style of attack, potentially cloaking "cyber-sabotage and industrial warfare" while extorting money from victims.

And they warn individuals are far from safe. The latest ransomware outbreak not only threatens to decimate their computers, but more criminals are establishing professional ransomware operations to hold victims' digital memories hostage.

They're not only employing call centres to help victims buy and hand over Bitcoins, but hiring translators for greater international reach.

They're even expanding their businesses with do-it-yourself ransomware kits that help criminals get their foot in the door, in what security experts fear will lead to an explosion in information theft.

One of the most devastating attacks was launched on Tuesday night, hitting Europe, and Ukraine in particular, hardest.

Known variously as Petya or Goldeneye, the malicious program shared elements of its attack with the WannaCry ransomware that infected thousands of computers worldwide in May.

Both used a stolen Microsoft Windows tool developed by the US National Security Agency to invade computers, though Dropsuite

01 Jul 2017
Daily Telegraph, Sydney

Author: Jennifer Dudley-nicholson • Section: General News • Article type : News Item
Audience : 235,091 • Page: 64 • Printed Size: 1060.00cm² • Market: NSW
Country: Australia • Words: 1083 • Item ID: 802540786

chief executive Charif El-Ansari says Goldeneye was "much worse" than its predecessor "for a couple of reasons".

The latest ransomware not only locked files on victims' computers but prevented the computer from being used at all. Goldeneye can also spread from one vulnerable computer, which did not receive the latest Microsoft updates, to any computer connected to it.

"If you have just one sick computer, it can quickly infect all computers across the network," El-Ansari says.

"Companies often have a strong defence on the outside but not a lot of defence inside."

It's this added sophistication that saw Goldeneye spread from the Ukraine to India, Denmark, Poland, the US and Spain.

In Australia — one of the world's biggest ransomware targets, according to Symantec — it mainly struck businesses with international links.

Computers at Cadbury's four Australian factories, for example, were infected by links to American parent company Mondelez International. Chocolate production stopped late on Tuesday and had restarted "in varying capacities" by Thursday thanks to manual overrides, according to spokeswoman Lainie Kirk.

The company, like others affected by the ransomware, has no solid deadline for returning to full capacity. And, in this case, paying criminals a ransom to get computers or data back isn't an option.

While the attackers asked for $391 in Bitcoin to be sent to their email address in return for a decryption key, their German provider suspended the account, cutting off their profits — as well as any hope of recovering victims' information.

Bitdefender senior e-threat analyst Bogdan Botezatu says Goldeneye could herald a dangerous new era for malware. "This is not commercial ransomware. It looks like it is meant to destroy. This is deliberately destroying user data," he says.

"This is the beginning because this proves ransomware can serve a double purpose: one is to make money for cyber-criminals, and one is to cloak cyber-sabotage or industrial warfare."

ESET's Nick FitzGerald describes Goldeneye as a "disk-crasher" that may have been designed to invade and destroy computers first, and demand money as a secondary goal. "(Being ransomware) was a mechanism to help hide the trail of a gang of cyber-terrorists or spies," he says.

"From a closer analysis of the code, it looks like its main intention was to trash the contents of computers."

Goldeneye also destroyed the "code of conduct" previously held by ransomware creators that instructed hackers to avoid targeting infrastructure or anything that could endanger a human life.

Despite their criminal behaviour, Botezatu says, ransomware makers often run their operations "like legitimate businesses".

"It's important for these criminals to build trust," he says. "They offer technical support so they can tell victims how to buy Bitcoins and therefore they make sure they get their Bitcoins. It's also important victims get their data back so others keep paying ransoms."

El-Ansari says some ransomware makers go so far as to employ a dedicated call centre to guide victims through the process of paying up. Other ransomware makers have been known to hire translators, particularly when sending scam emails to wealthy Scandinavian countries.

Ransomware writers are also using new strategies to expand their "businesses", such as selling do-it-yourself ransomware kits in return for a share of the money buyers extort from victims.

"Script kiddies are now able to put these attacks together," Botezatu says.

"You just fill in three parts and send it. It's possible to know nothing about code."

The latest DIY kit to surface on the dark web targeted Apple users for the first time, with MacRansom promising to encrypt up to 128 files on a Mac until a ransom was paid.

AsTech chief security strategist Nathan Wenzler says cyber-criminals are successfully extorting millions of dollars from victims, and they will keep doing it as long as a small portion of victims pay ransoms.

"Even if the ransom is relatively small, the sheer volume of these kinds of attacks can more than make up for it," he says.

"If the ransom is even only $100 that's well over a million dollars gained for a single attack. The ability to make large amounts of money even with relatively low success rates makes this an especially attractive attack method for cyber-criminals everywhere."

El-Ansari says DIY kits, along with high-profile attacks such as WannaCry and Goldeneye, will ensure ransomware becomes an even larger problem in Australia over the coming years.

Computer users should carefully consider their data security, he says, update their software, use an antivirus program and save all important information to an external source.

"Anyone can become a hacker and that's where we are right now," he says.

"Our response has to be more planned and more co-ordinated and we should start talking about 'security' rather than just 'cyber-security'."

"Script kiddies are now able to put these attacks together

e-threat analyst Bogdan Botezatu