NDS

Operations Security Group
Dec 1, 1997

To: Reuven Hasak
Roni Segoly
Ray Adams
John Norris

From: Avigail Gutman

Re: Global View - Dec. 1, 1997

Hello Gentlemen,

Following please find a summary of the information that has come in over the past several weeks. Due to the complexity of the [illegible]-confidential and cross-system relations between pirates I have grouped the information under four headings:
1 The active personas - an update
2. Holes, hacks and counter-measures
3. Operations
4. Clarification questions

As always, your comments and updates are welcome (and necessary towards filling the gaps, where they exist). Please comment on the structure of the report as well (there's always room for improvement)...

Avigail

The active personas - an update

DSS - Ron Ereiser's Group
Ron Ereiser's group hired Chris Tarnovsky to Calgary and tasked him to pick up where Pavel Donev, their in-house Bulgarian hacker, left off. Donev apparently managed to dump the card and use the code used by Marty Mullin. He apparently "signed" his cards differently (in the code) thus differentiating his cards from Mullin's.

Tarnovsky was tasked with creating four secure programmer boxes. Each member of the group will receive a box, thus enabling the programming of more cards and ensuring that if one of them gets caught - the business of selling 3Ms will continue.

The group refer to Tarnovsky as JOE.

NDS

Operations Security Group
Dec 1, 1997

To: Reuven Hasak
Roni Segoly
Ray Adams
John Norris

From: Avigail Gutman

Re: Global View - Dec. 1, 1997

Hello Gentlemen,

Following please find a summary of the information that has come in over the past several weeks. Due to the complexity of the cross-continental and cross-system relations between pirates I have grouped the information under four headings:
1 The active personas - an update
2 Holes, hacks and counter-measures
3. Operations
4. Clarification questions

As always, your comments and updates are welcome (and necessary towards filling the gaps, where they exist). Please comment on the structure of the report as well (there's always room for improvement)...

Avigail

The active personas - an update

DSS - Ron Ereiser's Group
Ron Ereiser's group hired Chris Tarnovsky to Calgary and tasked him to pick up where Pavel Donev, their in-house Bulgarian hacker, left off. Donev apparently managed to dump the card and use the code used by Marty Mullin. He apparently "signed" his cards differently (in the code) thus differentiating his cards from Mullin's.

Tarnovsky was tasked with creating four secure programmer boxes. Each member of the group will receive a box, thus enabling the programming of more cards and ensuring that if one of them gets caught - the business of selling 3Ms will continue.

The group refer to Tarnovsky as JOE.

The group has also been actively trying to recruit Oliver K. Ron Ereiser has called and emailed him and last week Tosh, Herb Huddlestone and Plamen Donev flew into Frankfurt and met with Oliver. At this meeting Donev and Oliver discussed Plamen's way to write into the P2 card, which they called "spoofing" or "glitching" and is a hardware break into the card. According to Alex, Donev explained to Oliver how he can control this process.

The Haifa team will look into this issue and provide a technical assessment.

(source: Mike, Alex)

The Bulgarians

Background summary: Several months ago, Ron Ereiser's group [illegible]is Tarnovsky to find a European hacker who could dump DSS [illegible] Tarnovsky turned to Jan Sagiorri, who in turn found Vesselin Nedeltchev and made the contact for the Canadian group. Nedeltchev brought Plamen Donev with him and the two were flown to the Cayman Islands and later to Canada and a California University lab to do the work.

At some point, Donev achieved the dump and broke off his partnership with Nedeltchev. From this point on, Donev became the in-house hacker for this group. Nedeltchev returned to Europe, where he remains in contact with Jan Sagiorri.

Present Situation: Sagiorri and Nedeltchev feel deceived by the Ereiser group and have said that the group owes them money. Nedeltchev recently visited with Sagiorri in Geneva.

(Note: A source in a Portuguese pirate card dealership claims there are two Bulgarians working on P11, one is [illegible]Ovranov, and the other - though unnamed - is said to have worked on the DSS hack.)

Plamen Donev is blamed with the group as the protege of Herb Huddlestone. He is described as reckless. Having suffered what was called "a meltdown" he flew back to Europe with Huddlestone.

Several calls were made from the Frankfurt Mariott Hotel to an area in Bulgaria. According to the Canadian group, Plamen is back in Bulgaria but is expected to return to Canada to work on an Un99 solution.

(The phone numbers of calls made from the hotel and credit card details have been entered into the Jerusalem Database. Ray is investigating these)

Both Mike and Alex assess that the Bulgarian duo are top-of-line hackers and could pose a threat to P11.

(Source: Mike, Alex, Angel)

PMK and Bill's group

PMK visited Canada. Discussion on IRC revealed that he met with some dealers and discussed options for marketing his device and making it compatible with P2 s/w. In addition, PMK's device-in-development, the MK13, is said to be prepped for a P2 ASIC.

More information will be provided by Ray.

Holes, Hacks and Counter Measures

DSS P2 ECM
On Nov. 21 at app. 16:30 in the afternoon, DTV launched an ECM which effectively 99'd all plastic 3M cards. Our information shows that Ereiser's group still hopes that Plamen Donev can come up with an un99 solution. The Internet [illegible] and IRC reveal disagreement on the possibility of un99ing P2 cards. Reactions are that the dealers in eastern Canada have acknowledged their inability to repair the dead cards while in western Canada efforts are being made to create an un99-tool.

DSS P2 - Operational pirate devices
At present the Batulator (by Norman Dick) and DDT cards (by Axa's group) are operational. Mike is in possession of a DDT card and will evaluate it for Jerusalem.

In addition, Internet websites report that next week dealers will send out 3M replacement cards to customers who have sent back their 99'd card with a working P2 and 50 CDN dollars.

An ECM against the plastic cards that are in the Batulator and the DDT card and an ECM to close down the holes that enable the production of these devices have been prepared and tested in Jerusalem.

DSS P2 - Other holes
To our knowledge two holes are being utilized by pirates to produce devices: the "09" and the "5A". While the current ECM has 99'd the 3M pirate cards, we Jerusalem knows has opened up another hole that, if discovered, could be utilized (in certain conditions) to produce a "blocker" device for P2
Although the issue has been discussed by Paul E. (the producer of the un99 box in P1) and Chris [illegible] we believe that less than a handful of people in the field could recognize this capability if they were made aware of the hole.

Jerusalem hopes to shut it down in the next ECM.
(source: Mike)

Galaxy Latin America
The holes found in DSS P2 are applicable to the Galaxy Latin America P1 card. We know that Norman Dick is working on hacking this system together with John Grayson and that Ron Ereiser's group has similar aspirations, though, to the best of our knowledge, Plamen has not yet begun working on the card.

We do not have information regarding the status of ND's work but we can assume he has found the 09 hole that enables the creation of a batulator type device (as this is the

product that he released for DSS P2). It is possible that he has not yet dumped the card to discover a way to retrieve the unique key - which would make the device financially worth marketing.

Pro-active measures to close down all known holes are in the planning stage and will be executed over the next month.

Sky P11
There is still no hack for Sky P11. The stories published on the Internet by McCormac, of a hack coming out of Ireland have been refuted by the UK group. Stories of a hack being developed by Bulgarians persist though no evidence of this work-in-progress has surfaced yet. We are hoping to use Mike's visit to Europe next month to gather more intelligence.

(Source: Angel, Alex)

Operations

Name	Project	Description	Status
P12 racket	Sky	Jerusalem is developing fake P12 cards that will be leaked into the field, to trap pirates to work on the wrong technology.	Appropriate chips are presently being sought.
Hannibal	Sky	Recruiting Hannibal as a source of information and liaising with the short-term purpose of discovering more information on [illegible] and towards using his contacts in the long-term. Recruitment will be considered after Mike's visit to Europe.	Angel has met with him. Hannibal has been found to be well-connected, but not a threat (neither a hacker nor a financier) to P11. A report has been submitted by Len.
Alex - Israel	Sky	Alex will visit in mid December to meet with staff and receive tasks concerning future Sky hacks	In planning.
Mike - Europe	Sky & DSS	Over Xmas Mike will meet with Hannibal and Birdy with the purpose of discovering more inf. regarding P11 status and finding out more information about the Bulgarians. Perhaps he will also meet Gary.	Avigail and Ray will prepare a brief and questions that need answers.

Dbl. Logging Chip	DSS	DSS P2 cards which contain an additional chip for logging the communication between any external device and the card. These cards will be used in operations wherein pirate s/w is being exhibited but not shared.	Nine cards have been printed and the chips embedded. Jerusalem is working on programming them.
Duck	DSS	DSS P2 ASIC "clone" on an FPGA has been produced. This can be used in a "show-and-tell" operation or to take a large order and cause the pirates financial grief. Jerusalem has many ways to kill this device.	Ready for use
Mike - Israel	DSS	Mike visited Israel to meet the staff, set working procedures with them and receive tasks	He is presently preparing for J. Johnny Walker Assessment of DDT card Further evaluation of card vulnerabilities.
Johnny Walker	DSS	New, secure pirate s/w will be implemented in North America. The s/w will be a program guarded by an external master smart-card. It will only produce a limited number of cards which can also be killed over	Mike is preparing under the direction of Jerusalem

Clarification questions:

- Who is Plamen Donev? Can we get more details about his whereabouts?
- Can we clarify the relationship between the Polish (DoctorQ or others?) and the Bulgarians?
- Do we have more information about the phone numbers called out of the hotel in Frankfurt: who was called? What was said?
- Will DoctorQ or Illian identify the second Bulgarian who is said to be working on P11?
- Are the replacement (DSS P2) 3M cards different from the ones that were ECM'd? Are they "un99'd"? Are they "fixed" so that they cannot be 99'd?