NDS

Operations Security Group
Dec 28, 1997

To: Reuven Hasak
Roni Segoly
Ray Adams
John Norris

From: Avigail Gutman

Re: Global View - December 28, 1997

The Active Personas - An Update

Ron Ereiser and Co.
Ron Ereiser received s/w for making batulators and two 3M cards (without s/w) from Chris Tarnovsky. As of mid-December, Ereiser had produced about 50 batulators. In addition, Plamen Donev produced a new 3M s/w for the group with which Ereiser has begun to program cards. However, it appears that the group will now be using Tarnovsky's s/w rather than Donev's, as it has "time-zone capabilities", while Donev's does not.

Donev has produced an unidentified device which the group is using. The group apparently has only one programmer which Donev has "booby-trapped" so that it cannot be opened and examined (or copied) by anyone.

Ereiser told Tarnovsky that for now, Donev is not working on anything for the group.

It seems Ereiser and the other members of the group are not together on the batulator deal (he is doing this on his own with Tarnovsky) but continue to cooperate where the 3M hack is concerned. (source: Mike)

Evaluation: It appears that Ereiser is drawing closer to Tarnovsky and may wish to rely on him more in the future. This is due to at least the following reasons:

1. Tarnovsky is better known (even predictable, as far as Ereiser is concerned), physically closer and speaks English;
2. He is a s/w expert who is as good as Donev (now that Ereiser believes he doesn't need a h/w expert, he can rely solely on Tarnovsky);
3. He is under the DSS footprint and can respond in real time;
4. He has a fuller understanding of the DSS system than Donev an
5. He is cheaper.

NDS

Operations Security Group
Dec 28, 1997

To: Reuven Hasak
Roni Segoly
Ray Adams
John Norris

From: Avigail Gutman

Re: Global View - December 28, 1997

The Active Personas - An Update

Ron Ereiser and Co.
Ron Ereiser received s/w for making batulators and blue 3M cards (without s/w) from Chris Tarnovsky. As of mid-December, Ereiser had produced about 50 batulators. In addition, Plamen Donev produced new 3M s/w for the group with which Ereiser has begun to program cards. However, it appears that the group will now be using Tarnovsky's s/w rather than Donev's, as it has "time-zone capabilities", while Donev's does not.

Donev has produced an un99 device which the group is using. The group apparently has only one programmer which Donev has "booby-trapped" so that it cannot be opened and examined (or copied) by anyone.

Ereiser told Tarnovsky that for now, Donev is not working on anything for the group.

It seems Ereiser and the other members of the group are not together on the batulator deal (he is doing this on his own with Tarnovsky) but continue to cooperate where the 3M hack is concerned. (source: Mike)

Evaluation: It appears that Ereiser is drawing closer to Tarnovsky and may wish to rely on him more in the future. This is due to at least the following reasons:

1. Tarnovsky is better known (even predictable, as far as Ereiser is concerned), physically closer and speaks English;
2. He is a s/w expert who is as good as Donev (now that Ereiser believes he doesn't need a h/w expert, he can rely solely on Tarnovsky);
3. He is under the DSS footprint and can respond in real time;
4. He has a fuller understanding of the DSS system than Donev and;
5. He is cheaper.

EX. 477

The Bulgarians
Reports from Europe indicated earlier this month that Plamen Donev and Vesselin Nedeltchev seem to have made their peace. Nedeltchev is in Bulgaria and in touch with Jan Sagiorri. Apparently Nedeltchev is the hardware expert and Donev the software expert. The two owe Sagiorri $5,000, each. While Nedeltchev had returned from Canada with $22,000 he did not pay back his debt to Sagiorri.

Plamen Donev is said to have worked out a means to "glitch" the DSS P2 card thus managing to un99 it. It has been said that he has the capability to control the glitching, which would give him an advantage with all chips. Since he left Canada he has created new 3M software and un99 software and a reader. Canadian sources say he is presently in Bulgaria and not working on anything for Erelser's group. (source: Alex, Mike)

Evaluation: If our information is correct and Nedeltchev is the h/w expert, it is possible that he may be called on again to handle the ASIC after the present P2 holes are closed. It is also worth following his activities (if any) in relation to P11.

Jan Sagiorri
Jan Sagiorri met with Chris Tarnovsky in Switzerland. According to Sagiorri, Oliver K. hacked P11. Sagiorri pulled out 22 P11s that he was given by Oliver K., three of which were clones, the rest enabled. Sagiorri intends to sell or trade in these cards. He has indicated that he has become quite close to Oliver K.

Sagiorri is presently working on D2Mac exclusively.

AXA and PGM
The two have copied the batulator code and have developed their own variation of the card which they call PASS (Plastic Automatic Subscription Simulator). The card is not generally available yet and is expected to be cheaper than the other combo-cards on the market. As you may recall - they were said to be behind the DDT cards as well, but denied it publicly. (source: Internet, Mike)

PMK
PMK has advertised the new MK13 device he has developed. The difference between this one and the previous version is that this one has a place for an 8-pin ASIC. PMK has said that he would not sell the MK13 but the schematics are on his web site should anyone wish to build one themselves. While his web site reports that he is working on the MK14, field operatives inform us that he is planning to add a pic chip to the MK12, into which he will write the batulator code. He thus hope to gain a slice of the North American pirate-card market. (source: U.S. unit, Internet)

Marty Mullin
No new information regarding Mullin's activities has come in over the past few weeks.

Holes Hacks and Counter Measures

DSS - operational devices

3M. Thus far there have been four types of 3M plastic pirate cards developed. The first two were hit by an ECM on November 21st and thrown into a 99 loop. The third was developed by Chris Tarnovsky and given to Ron Ereiser. The forth is the fix provided by Plamen Donev. (Ereiser has informed Tarnovsky that the group will begin to produce this card rather than Donev's)

The internet reports that Donev's 3M activates a virgin or subscribed plastic card but does not clear PPVs. However, anyone wishing to get PPVs can use the card in a DDT, ANON or P2B combo-card.

This card has not yet been evaluated either by Mike nor in Jerusalem as Mike is away and the card has been blocked so as to make dumping it a less obvious task. An ECM to shut down the hole that enables this kind of hack has been developed and should be launched sometime in January.

Clones. While we have not seen any as of yet, the internet reported that those clones that had become available lost most services in a short span of time.

Combos There are 5 kinds of combo cards on the market: the original batulators (two varieties) produced by Norman Dick, the DDT card which was said to be done by AXA (although he denies it), the ANON card done by an anonymous group, the PASS card also done by AXA and the newly released P2B - also by an unknown group.

The DDT, ANON and PASS are said to work with the Dallas 5000 chip while the P2B is said to be using the Dallas 5002.

Internet web sites warn that once the "hole" is closed over the air, these combo-cards will never work again. This indicates that at least some in the pirate community have an understanding of how this hack was achieved. An ECM for these has been tested and should be launched sometime in January. (source: Mike, internet)

UN99. We had heard of Donev's ability to "glitch" a card so as to achieve this effect earlier this month. Ereiser told Chris Tarnovsky that Donev has delivered a working un99 device. Meanwhile, there was talk that Dean Love (aka Fast Eddie) produced an UN99 device and was driving around Canada from dealer to dealer, fixing the dead cards for 35 dollars a card. Ereiser told Tarnovsky that his group has paid Fast Eddie 60,000 dollars - though it is not clear to what end. None of our field agents have received any of their

originally 99'd cards back from dealers to allow us to examine this futher. (source: Mike)

Blocker — There has been a rumor circulating for some weeks that a blocker device will become available soon. (source: Mike, U.S. unit)

Evaluation: It is generally agreed in Jerusalem (and by internet sources) that once the holes in the DSS P2 are closed in an ECM, the card's integrity will be restored. However, we should remain alert to the fact that the next step will probably be to crack the ASIC and produce a battery-type device.

Galaxy Latin America
A preemptive ECM will be launched in January to close down the holes that enable combo-card hacks to appear.

Sky Latin America
There have been rumors in Europe that Sky Latin America was being hacked. Some interest in this card was also manifested in a news group posting by PMK who described the card and asked if it has any resemblance to Sky P11.

Sky
The card remains un-hacked. Even rumors are scarce and far between.

Operations

Name	Project	Description	Status
P12 racket	Sky	Jerusalem is preparing fake P12 cards that will be leaked into the field, to get pirates to work on the wrong technology.	Appropriate chips are presently being sought.
Hannibal	Sky	Angel has met with him. Hannibal has been found to be well-connected, but not a threat. Mike says he is working on D2MAC only.	Pending Mike's full report re: P11 connection
Alex - Israel	Sky	Alex will visit in mid January, for technological tasking.	In planning (Chaim and Avigail)
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.	In preparation
	Sky	A similar card will be prepared for Sky P11	In planning

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. Roni will attempt to contact Marty with the offer through Pomella.
Mike - Israel	DSS	Mike visited Israel to discuss work in progress (Dec. 21-23)	He is presently preparing: 1. P3 disassembler and evaluation 2. Assessment new devices 3. Further evaluation of card vulnerability.
5000 cards	Sky	5000 cards that are "locked down" (can never be enabled) but appear legitimate (with a "please call..." message)	In preparation, Jerusalem will program the cards and send to the UK
TWIN	Sky	TWIN has spoken to both Andy Coulthurst and Josh Kamins who have submitted an evaluation.	Will be invited to Jerusalem for evaluation. He should not be hired before this takes place.
Pomella	DSS	The U.S. unit is seeking to catch Pomella and bring him to justice under U.S. law.	In preparation

Clarification Questions

- Any new information regarding Sky P11?
- Why is Plamen Donev not tasked to do anything further (GLA? P2 ASIC?)
- What is the origin of the card given by Oliver K. to Jan Sagiorri?
- What did FAST EDDIE get paid the 60,000 dollars for (exclusive rights to Ereiser's group? To undo their 99'd cards? Is he "neutralized"?)
- 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?
- Do we have any further information. on any Bulgarians or others working on P11?
- Who (if anyone) is working on the P2 ASIC? Where is Marty Mullin and what is he up to? What is Norman Dick up to?
- Is there any indication of a combo-card-type device out of Galaxy Latin America?

- Where did PMK get Sky Latin America cards? What is the interest here?