TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Andreas Jürimäe 178203IVCM

THE EFFECTIVENESS OF DMARC AND USAGE OF DMARC IN ESTONIAN GOVERNMENT INSTITUTIONS

Master's thesis

Supervisor: Kieren Nicolas Lovell
LT CDR RNorN RTD

Tallinn 2020

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Andreas Jürimäe 178203IVCM

DMARC’I EFEKTIIVSUS JA SELLE KASUTAMINE EESTI RIIKLIKES INSTITUTSIOONIDES

Magistritöö

Juhendaja: Kieren Nicolas Lovell
Kaptenmajor RNorN
RTD

Tallinn 2020

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Andreas Jürimäe

23.04.2020

Abstract

The purpose of this research paper is to analyse the current state of DMARC for public sector domains in Estonia. By analysing the state of DMARC recommendations can be made to strenghten the domains or show how well the DMARC mechanism is implemented.

To find out the implications of not using DMARC or using it incorrectly, 85 phishing and spam emails from Cambridge University were analysed. All of the emails were confirmed as phishing attempts so there were no false positives among the emails. The emails were divided into five categories – blackmail, credentials, personal data, malware and trust establishment. Also the sender and reply-to addresses were looked at and compared and the DMARC policy was extracted. By comparing the sender and reply-to addresses it was possible to deduce whether the sender address was spoofed. Another way of deciding whether the sender address was spoofed was to look at the headers of emails and checking where the emails really came from.

The analysis of the attacks in Cambridge University showed correlation between the attacks and usage of DMARC. The results showed that Estonian public sector domains should pay more attention to adopting DMARC and to the correct way of doing it.

This thesis is written in English and is 34 pages long, including 5 chapters, 8 figures and 1 table.

Annotatsioon

DMARC’i kasutamine Eesti riiklikes institutsioonides

Käesoleva magistritöö eesmärk on analüüsida Eesti avaliku sektori domeenide DMARC’i hetkeolukorda. Seda anlüüsides on võimalik teha soovitusi domeenide tugevdamiseks või tuua välja, kuidas DMARC on korrektselt seadistatud.

Et uurida, kui ohtlik võib olla DMARC’i mitte- või ebaefektiivselt kasutamine, analüüsiti 85 pahatahtlikku meili, mis olid pärit Cambridge’i ülikoolist. Kõikide analüüsitud meilide puhul oli nende pahatahtlikkus kinnitatud. Töö käigus jagati meilid viite kategooriasse – väljapressimine, kasutajaandmed, isikuandmed, pahavara ja usalduse tekitamine. Lisaks analüüsiti saatja ja vastuse aadresse ning uuriti välja DMARC’i tegutsemisviis. Saatja ja vastuse aadresse võrreldes oli võimalik järeldada, kas saatja aadress oli võltsitud. Võltsitud saatja aadressi tuvastamiseks oli võimalik ka meili päisest meili reaalset päritolu uurides.

Cambridge’i ülikoolist pärit pahatahtlike meilide analüüsimine näitas, et DMARC’i puudumine võimaldab domeene lihtsamalt ära kasutada. Eesti avaliku sektori domeenide puhul tuleks DMARC’i rohkem kasutusele võtta ning domeenide puhul, mis seda juba kasutavad, DMARC’i tegutsemisviisi karmimaks muuta.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 34 leheküljel, 5 peatükki, 8 joonist ja 1 tabelit.

List of abbreviations and terms

CamCERT	University of Cambridge Computer Emergency Response Team
CERT	Computer Emergency Response Team
CUDN	Cambridge University Data Network
NIST	National Institute of Standards and Technology
DNS	Domain Name System

Table of contents

List of figures

List of tables

1 Introduction

Using email for communicating is a regular part of our lives. The problem is that email itself is not a very secure way of communicating [1]. However, it is an extremely popular way of official communication which makes a case of misuse very likely. Estonia is known for its digital society and e-services [2]. This kind of mentality can make people more trusting towards official government websites and domains. When this trust is coupled with minimal or no measures for domain security – DMARC in this case – then the likelihood of a successful misuse could be high.

DMARC is a mechanism that allows to check the authenticity of a domain of an incoming email. It does this by using DNS txt records and two other mechanisms. The DNS record specifies the policy on how to deal with emails that fail checks for the domain. The two other mechanisms are SPF and DKIM. SPF uses DNS txt record to specify allowed IP addresses for mail to originate from and DKIM uses DNS txt record to publish the domain's public key. This key is used to validate a cryptographic signature for the email.

To find out what role DMARC has in successful phishing attacks I got access to emails related to spam and phishing attacks against Cambridge University email addresses. Analysing the emails gives a picture whether and how DMARC was used in those cases. I will be doing a manual data analysis because the existing methods that are used to identify spam did not work for these emails.

The result of this thesis is recommendations to Estonian government domain owners whether or how they should change their DMARC implementation.

2 Literature overview

When searching for relevant literature on the subject I came across on different papers and articles but none of them were papers about the efficiency of DMARC.

Two of the findings [3], [4] were articles about email security in general. They described how email is a very widely used means of communication but how security has not been one of the things thought about when the technology was created. In the articles DMARC is mentioned as a way to try and fix that mistake by allowing to verify domains when sending emails.

Two more findings [5], [6] were patent and paper about classification of emails. The patent [5] described a system which uses a classification server that determines if an email is legitimate or not based on different characteristics of an email. One of the characteristics that is being looked at is DMARC which is used to determine whether the sender owns the domain or not. The paper [6] described a service that scans websites and gives scores based on the privacy and security properties of those websites. DMARC is used to calculate the score of a website.

Some of the findings were papers about different ways to fight phishing attacks. Papers [3] and [7] were two examples of that. Paper [3] talked about fighting phishing and securing data with email authentication and one of the ways to authenticate email is using DMARC. It is said in the paper that using email authentication could help a lot against these kinds of attacks. Paper [7] described general technical ways to improve the security of email communications. DMARC was mentioned as a recommendation.

Rest of the findings [8], [9], [10] were papers about adoption of anti-spoofing protocols in email systems. The papers looked and analysed how much is DMARC used in real systems and why it is used as little as it is. They have done interviews with system administrators to find out why DMARC is not used more.

Finding [8] describes very well how and why DMARC is used as little as it is. It turns out that among Alexa top 1 million domains only 1% use DMARC and 40% use SPF. In the paper they asked system administrators the following questions. First, they asked how they usually detect spoofing attempts. Then they wanted administrators to comment on the value and potential weaknesses of SPF, DKIM and DMARC. After that they asked about personal perceptions towards under-adoption of anti-spoofing protocols and the possible reasons. Lastly, they wanted comments on the possible solutions moving forward to the email spoofing problem. The results were grouped into six main topics. The weaknesses were technical defects of the protocols, lack of critical mass, benefits not significantly overweighing costs, deployment difficulties in practice, risks of breaking the existing system and finally solutions moving forward.

The technical defects consisted of problems when using mail forwarding or mailing lists which removes the original sender IP and thus SPF check will fail. Another technical defect was to do with identifier alignment which allows an attacker to change the displayed ‘from’ field into something that the receiver trusts but keep the field containing real sender address as something else which will pass the checks.

Lack of critical mass means that while only a small number of domains are publishing their SPF and DMARC record others will not hurry to do the same because the benefits are not large enough.

In general system administrators feel that the benefits do not significantly overweigh the costs. What’s even more, non-email domains do not get enough benefits at all.

Two more weaknesses that are keeping system administrators from using SPF, DKIM and DMARC are deployment difficulties in practice and risks of breaking the existing system. That is because real systems might be very large and consisting of many subsystems which makes the set up more difficult than in the simple textbook cases.

Presented solutions moving forward were more education of the users and using security indicators or visual cues on the email client like the ones that are used in web browsers when indicating the validity of SSL certificates. Most of the system administrators thought that automatic detection systems could not fully prevent spoofing.

It seems that there has been research on how much DMARC is used and why DMARC should be used. I intend to see what role DMARC plays in real phishing attacks and if it seems to be effective in real cases. I also intend to look at real DMARC configurations and see how different organizations have set it up. (Having a misconfigured DMARC is not doing any good).

3 DMARC

DMARC stands for Domain-based Message Authentication, Reporting, and Conformance. It is a mechanism which can be used by a mail-originating organization to express domain-level policies and preferences for message validation, disposition, and reporting [11, p. 1].

3.1 Introduction

For DMARC to work, two methods are used to provide domain-level authentication. These methods are The Sender Policy Framework (SPF) and Domain Keys Identified Mail (DKIM) [11, p. 3].

The basic outline for procedure is the following. The domain owner publishes a DMARC policy for their domain. When an email is received from that domain according to the 'From' field of Internet Message Format [12] then the SPF and DKIM checks are made. If the checks fail, then the specified DMARC policy is followed for that email. That could mean sending it to spam folder or rejecting it. After that the receiver sends feedback to the domain owner about mail claiming to be from their domain [11, p. 4].

DMARC is designed to help combat phishing attacks that claim to come from legitimate senders [11, p. 7]. Also, the DMARC mechanism has been found to help with creating reliable and defensible message streams [11, p. 7]. By doing that, it becomes more difficult for scammers to use familiar and otherwise safe brands for their benefit.

3.2 SPF

SPF stands for Sender Policy Framework. Domain owners can create SPF records to specify which hosts are permitted to use their domain name and mail receivers can use those records to test the authenticity of incoming mail [13, p. 5]. An SPF record is a DNS record. The SPF record is expressed as text found in a DNS TXT resource record [13, p.

11]. Based on the result of the SPF check the receiver can decide what to do with the email. For example, they can choose to send it to spam or reject it.

3.3 DKIM

DKIM stands for DomainKeys Identified Mail. Domain owner can claim some responsibility for a message by associating the domain with the message [14, p. 1]. This association is validated using a cryptographic signature by querying the signer's domain for the public key [14, p. 4]. It does not need its own key management system and can be used with the existing mail infrastructure [14, pp. 4-5].

3.4 Domain matching

DMARC uses the 'From' field of the Internet Message Format [12] to get the domain to query further. This field is used because it is a required message header field and therefore guaranteed to be present in compliant messages [11, p. 9].

3.4.1 DKIM domain matching

DMARC permits domain matching of the DKIM field in two ways, strict or relaxed [11, p. 9]. In relaxed mode, the domains specified in the signature and From field do not have to match exactly [11, p. 10]. The domain received from the From field can contain the domain gotten from the signature [11, p. 10]. In strict mode, only an exact match between the Fully Qualified Domain Names (FQDNs) is allowed [11, p. 10]. Domain matching is needed because a single message can bear a valid signature from any domain [11, p. 10].

3.4.2 SPF domain matching

DMARC permits domain matching for SPF in two ways, strict or relaxed [11, p. 10]. In relaxed mode, the domains do not have to match exactly but in strict mode the match must be exact in order to count a SPF check as valid [11, p. 11].

3.5 Policies

There are three policies for domain owners to choose from. These are the following: 'none', 'quarantine' and 'reject' [11, p. 18]. 'None' means that the domain owner has no specific requests for any action to be taken [11, p. 18]. 'Quarantine' means that the domain owner wants the email that fails the check to be treated as suspicious which could mean placing the email to spam folder, scrutinizing it with additional intensity or flagging as suspicious [11, p. 18]. ‘Reject’ means the domain owner does not want the email to reach the recipient if it fails the check [11, p. 18].

Using the strictest policy could seem the best option since it means that if there is even the chance that the email is spoofed the email is rejected and never reaches the recipient. However, it also means that in case of false positives you also have emails that should get thru but do not.

Using the ‘quarantine’ policy gives more control to the recipient. Depending on how the email is handled it is the recipient’s decision whether they look thru their spam folder or emails flagged as suspicious. The ‘quarantine’ policy could also mean that the postmaster needs to check those emails but that would probably need a lot of manpower and there could be a problem with confidentiality.

Using the most relaxed policy gives all the control to the recipient. However, since the ‘none’ policy does not specify anything in case of a check failure it has the same efficiency as having no DMARC record at all.

3.6 Feedback

DMARC allows to specify email addresses to send feedback so that domain owners can see what effect their policies are having [11, p. 28]. These addresses are specified in the ‘ruf’ and ‘rua’ tags [11, pp. 19-20]. If the domain from the ‘From’ field does not match the domain from an email address that is specified for feedback then the external destination will need to be verified [11, p. 28]. If the domain in the feedback address is not verified, then no feedback will be sent to that address.

3.7 Security implications

Not using DMARC or using it in a way that is not fully taking advantage of the possibilities has certain security implications.

If DMARC is not used, then it is possible to spoof the ‘from’ address which allows anyone to pretend to become someone else in an email. An attacker could pretend to send malware masqueraded as an invoice from an email of a respected company.

There is also the possibility that a relaxed policy is used which in turn allows for a chance that a malicious email can get thru. For example, when ‘none’ is used as a policy and a check fails then the domain owner has given the order to do nothing. So, despite failing a check nothing is being done with the email.

Another thing that might happen is misconfiguring email addresses for the feedback routine. If the feedback address is from a different domain then the receiving domain must verify that it allows for the feedback to arrive from the original domain. If this is not done or is done incorrectly then the original domain owner might think that they are monitoring what goes on with their domain but in actuality no emails about misuses are coming thru.

Using DMARC with ‘none’ policy also has effect on the spam score. Automatic checking systems might lower the spam score just because a DMARC record is present.

3.8 DMARC usage in Estonia in 2019

I chose thirteen .ee domains that could be used with bad intentions. ˇ

In the following chapter I will show the DMARC records and explain the meaning of different parts of the records. For the reader to understand better I will go over the parameters used in DMARC records.

- v – Version tag. It identifies the record as a DMARC record and it must have the value of ‘DMARC1’ [11, p. 20].
- p – Policy tag. It indicates the policy to be enacted and it applies to the domain queried and to subdomains unless the policy for the subdomain is also specified. Possible values are ‘none’, ‘quarantine’ and ‘reject’ [11, p. 18].
- sp – Subdomain policy tag. It indicates the policy to be enacted on the subdomains of the queried domain. Possible values are identical to the values of the policy tag [11, p. 20].

- pct – Percentage tag. It indicates the percentage of messages to which the DMARC policy is to be applied [11, pp. 18-19].

- fo – Failure reporting options tag. It provides options for generation of failure reports. The value for the tag is a colon-separated list of allowed characters that indicate reporting options. The possible values are *0, 1, d, s*. *0* or *1* means that a DMARC failure report should be generated depending on whether all or any underlying authentication mechanism has produced a failure accordingly. *d* means that a DKIM failure report should be generated in case of a DKIM specific failure. *s* means that an SPF failure report should be generated in case of a SPF specific failure [11, p. 18].

- rua – Aggregate feedback addresses tag. It specifies the addresses to which aggregate feedback is to be sent [11, pp. 19-20].

- ruf – Message-specific failure feedback addresses tag. It specifies the addresses to which message-specific failure feedback is to be sent [11, p. 20].

- aspf – SPF alignment tag. It indicates whether strict or relaxed alignment mode is required by the domain owner. Possible values are *r* or *s* [11, p. 17].

- adkim – DKIM alignment tag. It indicates whether strict or relaxed alignment mode is required by the domain owner. Possible values are *r* or *s* [11, p. 17].

- rf – Message-specific failure report format tag. It specifies the report format to use when a message fails both SPF and DKIM tests to report details of the individual failure. The default value is *afrf* [11, p. 19].

- ri – Aggregate report interval tag. It indicates a request to generate aggregate reports separated by no more than the requested number of seconds. The default value is 86400 [11, p. 19].

For example, the following DMARC record would have the following properties.

v=DMARC1; p=quarantine; rua=mailto:rua.feedback@test.com; ruf=mailto:ruf.feedback@test.com; fo=1; aspf=s; pct=25; sp=reject;

The policy for main domain is ‘quarantine’ and the policy for subdomains is ‘reject’. Email address for aggregate feedback is rua.feedback@test.com and email address for message specific feedback is ruf.feedback@test.com. DMARC policy should be enacted on one in every four emails concerning the domain. When doing the SPF check the domains should match exactly as described by ‘aspf’ tag’s value. Failure report should be generated if any of the checks fail as described by ‘fo’ tag’s value.

3.8.1 Eesti.ee

The domain eesti.ee is a webpage that collects and shows information about the citizen. The information is queried from various government institutions. It also allows citizens to use different e-services for actions that would otherwise require people to go to a physical location. Furthermore, it creates an email address for every citizen and forwards all incoming email traffic to the one specified by the citizen which makes it a create way to launch phishing attacks. The domain has the following DMARC record.

v=DMARC1; p=none; sp=none; pct=100; fo=1; rua=mailto:dmarc-rua@ria.ee,mailto:h6gl0kat@ag.dmarcian-eu.com; ruf=mailto:dmarc-ruf@ria.ee;

From the record we can see that the policy is set to ‘none’ which means that all emails from that domain reach their recipients. However, ‘rua’ and ‘ruf’ tags specify email addresses to send feedback if SPF or DKIM checks fail [11, pp. 19-20]. In this case, only the second address specified in the ‘rua’ tag receives the feedback. The first address in the ‘rua’ tag and the address in the ‘ruf’ tag are not verified external destinations.

3.8.2 Ministry of Justice

The domain for Estonian Ministry of Justice is just.ee. It has the following DMARC record.

v=DMARC1; p=none; sp=none; rua=mailto:dmarc-reports@dmarc.rik.ee,mailto:re+kqetny45ejl@dmarc.postmarkapp.com; ruf=mailto:dmarcfail@just.ee; rf=afrf; pct=100; fo=1; ri=86400

From the record we can see that the policy is set to ‘none’ which means that all emails from that domain reach their recipients. However, ‘rua’ and ‘ruf’ tags specify email addresses to send feedback if SPF or DKIM checks fail.

3.8.3 Ministry of Defence

The domain for Estonian Ministry of Defence is kaitseministeerium.ee. It does not have a DMARC record. It does however have an SPF record which looks like this.

v=spf1 a mx ip4:188.0.48.32/32 ip4:188.0.48.99/32 -all

By not having a DMARC record there are no guidelines from the domain owner on how to handle spoofed or otherwise suspicious emails from their domain. Thanks to the SPF record there is at least the possibility to check for the legitimacy of the origin of the email.

3.8.4 Ministry of Economic Affairs and Communications

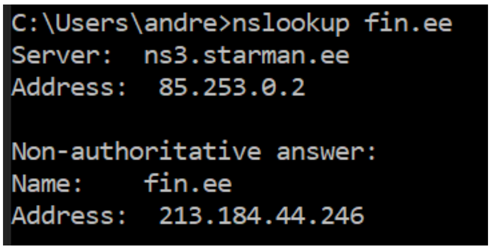
The domain for Estonian Ministry of Economic Affairs and Communications is mkm.ee. It has the following DMARC record.

v=DMARC1; p=none; sp=none; rua=mailto:dmarcaggr@rik.ee; rf=afrf; pct=100; ri=86400

From the record we can see that the policy is set to 'none' which means that all emails from that domain reach their recipients. However, 'rua' tag specifies an email address to send general feedback to.

3.8.5 Ministry of Finance

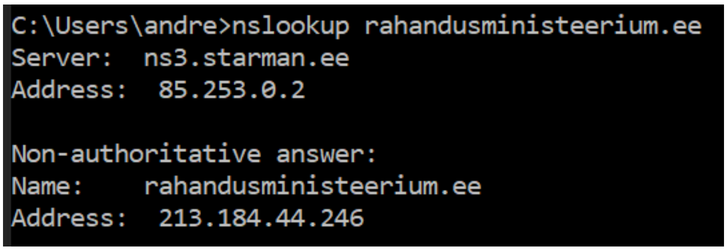
There seem to be two domains for the Estonian Ministry of Finance. These are fin.ee and rahandusministeerium.ee. The first one gets redirected to the second one. That can be seen by the output of command nslookup where address is same for both domains as seen in Figure 1 and in Figure 2.



```
C:\Users\andre>nslookup fin.ee
Server:  ns3.starman.ee
Address:  85.253.0.2

Non-authoritative answer:
Name:    fin.ee
Address:  213.184.44.246
```

Figure 1. Nslookup output for fin.ee.



```
C:\Users\andre>nslookup rahandusministeerium.ee
Server:  ns3.starman.ee
Address:  85.253.0.2

Non-authoritative answer:
Name:    rahandusministeerium.ee
Address:  213.184.44.246
```

Figure 2. Nslookup output for rahandusministeerium.ee.

That might be caused by changing the domain but leaving the old domain to work beside the new one. On the contacts page for the Ministry of Finance all the personal email addresses for their employees have the ending fin.ee and only one email address has the domain rahandusministeerium.ee at the end [15].

There is no DMARC record for fin.ee but there is one for rahandusministeerium.ee which looks like this.

v=DMARC1; p=none; pct=100; rua=mailto:dmarc.reports@rmit.ee,mailto:re+svuaw6h5ru6@dmarc.postmarkapp.com ; sp=none; aspf=r;

From the record we can see that the policy is set to ‘none’ which means that all emails from that domain reach their recipients. However, ‘rua’ tag specifies an email address to send general feedback to. In this case, feedback is sent only to the second email address because the first one is not a verified external destination.

The fact that there is no DMARC record for fin.ee may seem fine if the domain is no longer used. However, the domain still redirects to rahandusministeerium.ee which could have a negative effect. If someone receives an email from fin.ee which is spoofed and the contents seem to be from the Ministry of Finance then visiting page fin.ee would convince the recipient in the legitimacy of the email.

3.8.6 Ministry of the Interior

The domain for Estonian Ministry of the Interior is siseministeerium.ee. It has no DMARC record. It does however have an SPF record which looks like this.

v=spf1 include:spf.smit.ee ip4:213.180.8.75 -all

By not having a DMARC record there is no guidelines from the domain owner on how to handle spoofed or otherwise suspicious emails from their domain. Thanks to the SPF record there is at least the possibility to check for the legitimacy of the origin of the email.

3.8.7 Police

In Estonia the police are responsible for public safety but also for issuing identification documents. This includes passports and Estonian ID cards which are used to digitally sign documents. That makes the domain a potential target for malicious use. The domain for Estonian Police is politsei.ee. It has no DMARC record. It does however have a SPF record which looks like this.

v=spf1 include:spf.smit.ee -all

By not having a DMARC record there is no guidelines from the domain owner on how to handle spoofed or otherwise suspicious emails from their domain. Thanks to the SPF record there is at least the possibility to check for the legitimacy of the origin of the email.

3.8.8 Estonian Defence Forces

The domain for Estonian Defence Forces is mil.ee. It has the following DMARC record.

v=DMARC1; p=none; ruf=mailto:postmaster@mil.ee;

From the record we can see that the policy is set to ‘none’ which means that all emails from that domain reach their recipients. However, ‘ruf’ tag specifies an email address to send general feedback to.

3.8.9 Tax and Customs Board

The domain for Estonian Tax and Customs Board is emta.ee. It has the following DMARC record.

v=DMARC1; p=none; pct=100; rua=mailto:dmarc.reports@rmit.ee,mailto:re+dvexjytwvah@dmarc.postmarkapp.com; sp=none; aspf=r;

From the record we can see that the policy is set to ‘none’ which means that all emails from that domain reach their recipients. However, ‘rua’ tag specifies an email address to send general feedback to. In this case, feedback is sent only to the second email address because the first one is not a verified external destination.

3.8.10 Centre of Registers and Information Systems

The domain for Estonian Centre of Registers and Information Systems is rik.ee. It has the following DMARC record.

v=DMARC1; p=none; sp=none; rua=mailto:dmarc-reports@dmarc.rik.ee; ruf=mailto:dmarcfail@just.ee; rf=afrf; pct=100; fo=1; ri=86400

From the record we can see that the policy is set to ‘none’ which means that all emails from that domain reach their recipients. However, ‘rua’ and ‘ruf’ tags specify email addresses to send general feedback to.

3.8.11 Information System Authority

The domain for Estonian Information System Authority is ria.ee. It has the following DMARC record.

v=DMARC1; p=none; sp=none; pct=100; fo=1; rua=mailto:dmarc-rua@ria.ee,mailto:fn8muqll@ag.dmarcian-eu.com; ruf=mailto:dmarc-ruf@ria.ee;

From the record we can see that the policy is set to ‘none’ which means that all emails from that domain reach their recipients. However, ‘rua’ and ‘ruf’ tags specify email addresses to send general feedback to.

3.8.12 NATO Cooperative Cyber Defence Centre of Excellence

The domain for NATO Cooperative Cyber Defence Centre of Excellence is ccdcoe.org. It does however have a SPF record which looks like this.

v=spf1 a mx ip4:188.0.48.32/32 ip4:188.0.48.99/32 -all

By not having a DMARC record there is no guidelines from the domain owner on how to handle spoofed or otherwise suspicious emails from their domain. Thanks to the SPF record there is at least the possibility to check for the legitimacy of the origin of the email.

There is also a domain ccdcoe.ee which redirects users to ccdcoe.org. Ccdcoe.ee has the following DMARC record.

v=DMARC1; p=reject; sp=reject; pct=100; fo=1; rua=mailto:dmarc@ccdcoe.ee; ruf=mailto:dmarc@ccdcoe.ee

From the record we can see that the policy is set to 'reject' which means that the emails that fail a check get dropped and they do not reach the recipient. 'Rua' and 'ruf' tags specify email addresses to send feedback to. However, the email addresses on the contacts page all use the domain ccdcoe.org [16] which means that they are probably also sending their email from ccdcoe.org domain. This seems to be the opposite situation to the Ministry of Finance one where the main domain has a DMARC record and the one that is redirecting to the main domain has no DMARC record. But in this case it allows to abuse the main domain directly.

3.8.13 Conclusions

I chose thirteen domains but ended up analysing fourteen because the Ministry of Finance and CCDCOE had two domains that were working and pointing to the same page.

Out of those fourteen, nine had a DMARC record. However, all but one of them had 'none' set as their policy which means that they are only monitoring their domain thru feedback sent back to them by the recipient's mail service providers. Three of those domains had problems with their external destinations. Eesti.ee, rahandusministeerium.ee and emta.ee had a feedback email address that was not authorized to receive feedback from the domain. Fortunately, they had at least one other email address set to receive feedback.

Five of the domains had no DMARC record. Despite that they at least had an SPF record which can be used to check the legitimacy of an email whether the domain has a DMARC record or not.

The most important conclusion from analysing these domains is the discovery about the Ministry of Finance which has two working domains, rahandusministeerium.ee and fin.ee, that point to the same IP address but only one of which has a DMARC record. That allows to use the domain fin.ee, the one without a DMARC record, to send emails with spoofed ‘from’ addresses. When the potential victim tries to visit page www.fin.ee then they are sent to page www.rahandusministeerium.ee which can act as a convincer. If the potential victim suspects that www.fin.ee has been set up by an attacker and is just made to redirect visitors to www.rahandusministeerium.ee then it can be seen by using the tool nslookup that both domains point to the same IP address which acts also as a good convincer.

3.9 DMARC in Estonia in 2020

To see if domain owners had improved their DMARC records I checked the same domains again and this time added 6 other government domains to the list.

3.9.1 Eesti.ee

Eesti.ee has the following DMARC record.

v=DMARC1; p=reject; sp=reject; pct=100; fo=1; rua=mailto:dmarc-rua@ria.ee,mailto:grwm9pu4@ag.dmarcian-eu.com; ruf=mailto:dmarc-ruf@ria.ee;

From the record we can see that the policy is set to ‘reject’ which means that the emails that fail a check get dropped and they do not reach the recipient. Both feedback addresses are verified external destinations.

3.9.2 Ministry of Justice

The domain for Estonian Ministry of Justice is just.ee. It has the following DMARC record.

v=DMARC1; p=reject; sp=reject; rua=mailto:dmarc-reports@dmarc.rik.ee; rf=afrf; pct=100; fo=1

From the record we can see that the policy is set to ‘reject’ which means that the emails that fail a check get dropped and they do not reach the recipient. The specified feedback address is a verified external destination.

3.9.3 Ministry of Defence

The domain for Estonian Ministry of Defence is kaitseministeerium.ee. It has the following DMARC record.

v=DMARC1; p=reject; sp=reject; rua=mailto:dmarc-reports@dmarc.rik.ee; rf=afrf; pct=100; fo=1

From the record we can see that the policy is set to 'reject' which means that the emails that fail a check get dropped and they do not reach the recipient. The specified feedback address is a verified external destination.

3.9.4 Ministry of Economic Affairs and Communications

The domain for Estonian Ministry of Economic Affairs and Communications is mkm.ee. It has the following DMARC record.

v=DMARC1; p=none; sp=none; rua=mailto:mkm_dmarc@mnt.ee; rf=afrf; pct=100; ri=86400

From the record we can see that the policy is set to 'none' which means that all emails from that domain reach their recipients. The feedback address specified by the 'rua' tag is not verified so feedback will not reach the recipient.

3.9.5 Ministry of Finance

There seems to be two domains For the Estonian Ministry of Finance. These are fin.ee and rahandusministeerium.ee which both point to the same IP address. Both domains have a DMARC record. Rahandusministeerium.ee has the following DMARC record.

v=DMARC1; p=none; pct=100; rua=mailto:dmarcaggr@just.ee; ruf=mailto:dmarcfail@just.ee; sp=none; aspf=r;

From the record we can see that the policy is set to 'none' which means that all emails from that domain reach their recipients. Both feedback addresses are verified external destinations which means that at least the domain owner will be informed about attempts to misuse the domain.

Fin.ee has the following DMARC record.

v=DMARC1; p=none; sp=none; rua=mailto:dmarcaggr@just.ee; ruf=mailto:dmarcfail@just.ee; rf=afrf; pct=100; fo=1; ri=86400

From the record we can see that the policy is set to ‘none’ which means that all emails from that domain reach their recipients. Both feedback addresses are verified external destinations which means that at least the domain owner will be informed about attempts to misuse the domain.

3.9.6 Ministry of the Interior

The domain for Estonian Ministry of the Interior is siseministeerium.ee. It has the following DMARC record.

v=DMARC1; p=reject; rua=mailto:DMARC-r@smit.ee; ruf=mailto:DMARC-r@smit.ee; sp=none; fo=1; pct=100

From the record we can see that the policy is set to ‘reject’ and the policy for subdomains is set to ‘none’ which means that emails originating from the main domain that fail a check get dropped and emails originating from the subdomains reach the recipients. Neither feedback address is a verified external location.

3.9.7 Police

The domain for Estonian Police is politsei.ee. It has the following DMARC record.

v=DMARC1; p=reject; rua=mailto:DMARC-r@smit.ee; ruf=mailto:DMARC-r@smit.ee; sp=none; fo=1; pct=100

From the record we can see that the policy is set to ‘reject’ which means that the emails that fail a check get dropped and they do not reach the recipient. Neither feedback address is a verified external location.

3.9.8 Estonian Defence Forces

The domain for Estonian Defence Forces is mil.ee. It has the following DMARC record.

v=DMARC1; p=quarantine; sp=reject; pct=100; ruf=mailto:postmaster@mil.ee;

From the record we can see that the policy is set to ‘quarantine’ and the policy for subdomains is set to ‘reject’ which means that emails originating from the main domain that fail a check get flagged or sent to spam folder and emails originating from the subdomains get dropped. The feedback address is a verified external destination.

3.9.9 Tax and Customs Board

The domain for Estonian Tax and Customs Board is emta.ee. It has the following DMARC record.

v=DMARC1; p=reject; pct=100; rua=mailto:dmarc.reports@rmit.ee,mailto:re+dvexjytwvah@dmarc.postmarkapp.com; sp=reject; aspf=r;

From the record we can see that the policy is set to ‘reject’ which means that the emails that fail a check get dropped and they do not reach the recipient. The feedback address ending with *rmit.ee* is not a verified external destination so it will not receive any feedback information.

3.9.10 Centre of Registers and Information Systems

The domain for Estonian Centre of Registers and Information Systems is rik.ee. It has the following DMARC record.

v=DMARC1; p=reject; sp=reject; rua=mailto:dmarc-reports@dmarc.rik.ee; rf=afrf; pct=100; fo=1

From the record we can see that the policy is set to ‘reject’ which means that the emails that fail a check get dropped and they do not reach the recipient. The feedback address is a verified external destination.

3.9.11 Information System Authority

The domain for Estonian Information System Authority is ria.ee. It has the following DMARC record.

v=DMARC1; p=reject; sp=reject; pct=100; fo=1; rua=mailto:dmarc-rua@ria.ee,mailto:fn8muqll@ag.dmarcian-eu.com; ruf=mailto:dmarc-ruf@ria.ee;

From the record we can see that the policy is set to ‘reject’ which means that the emails that fail a check get dropped and they do not reach the recipient. The feedback addresses are verified external destinations.

3.9.12 NATO Cooperative Cyber Defence Centre of Excellence

The domain for NATO Cooperative Cyber Defence Centre of Excellence is ccdcoe.org. It has the following DMARC record.

v=DMARC1;p=quarantine;sp=reject;ruf=mailto:dmarc-ruf@ccdcoe.org;

From the record we can see that the policy is set to ‘quarantine’ and the policy for subdomains is set to ‘reject’ which means that emails originating from the main domain that fail a check get flagged or sent to spam folder and emails originating from the subdomains get dropped. The feedback address is a verified external destination.

There is also a domain ccdcoe.ee which redirects users to ccdcoe.org. Ccdcoe.ee has the following DMARC record.

v=DMARC1; p=reject; sp=reject; pct=100; fo=1; rua=mailto:dmarc@ccdcoe.ee; ruf=mailto:dmarc@ccdcoe.ee

From the record we can see that the policy is set to ‘reject’ which means that the emails that fail a check get dropped and they do not reach the recipient. The feedback addresses are verified external destinations.

3.9.13 Ministry of Education and Research

The domain for Estonian Ministry of Education and Research is hm.ee. It has the following DMARC record.

v=DMARC1; p=reject; sp=reject; rua=mailto:dmarc-reports@dmarc.rik.ee; rf=afrf; pct=100; fo=1

From the record we can see that the policy is set to ‘reject’ which means that the emails that fail a check get dropped and do not reach the recipient. The feedback address is a verified external destination.

3.9.14 Ministry of the Environment

The domain for Estonian Ministry of the Environment is envir.ee. It has the following DMARC record.

v=DMARC1; p=none; rua=mailto:dmarcAggregate@envir.ee; ruf=mailto:dmarcForensic@envir.ee; fo=1; adkim=s; aspf=s;

From the record we can see that the policy is set to ‘none’ which means that all emails from that domain reach their recipients. The feedback address is a verified external destination.

3.9.15 Ministry of Culture

The domain for Estonian Ministry of Culture is kul.ee. It has the following DMARC record.

v=DMARC1; p=reject; pct=100; rua=mailto:dmarc.reports@rmit.ee,mailto:re+ltexqsonrhe@dmarc.postmarkapp.com; sp=reject; aspf=r;

From the record we can see that the policy is set to ‘reject’ which means that the emails that fail a check get dropped and do not reach the recipient. The feedback address specified by the ‘rua’ tag is not verified so feedback will not reach the recipient.

3.9.16 Ministry of Rural Affairs

The domain for Estonian Ministry of Rural Affairs is agri.ee. It has the following DMARC record.

v=DMARC1; p=reject; rua=mailto:postmaster@agri.ee; ruf=mailto:postmaster@agri.ee; sp=none; fo=1

From the record we can see that the policy is set to ‘reject’ and the policy for subdomains is set to ‘none’ which means that emails originating from the main domain that fail a check get dropped and emails originating from the subdomains reach their recipient. The feedback address is a verified external destination.

3.9.17 Ministry of Social Affairs

The domain for Estonian Ministry of Social Affairs is sm.ee. It has the following DMARC record.

v=DMARC1; p=none; sp=none; pct=100; fo=1; rua=mailto:dmarc@tehik.ee,mailto:re+qagovn3gfze@dmarc.postmarkapp.com; ruf=mailto:dmarc.afrf@tehik.ee

From the record we can see that the policy is set to ‘none’ which means that all emails from that domain reach their recipients. The feedback addresses with domain tehik.ee specified by the ‘rua’ and ‘ruf’ tags are not verified so feedback will not reach these recipients. However, feedback address with domain dmarc.postmarkapp.com is a verified external destination.

3.9.18 Ministry of Foreign Affairs

The domain for Estonian Ministry of Foreign Affairs is vm.ee. It has no DMARC record. It does however have a SPF record which looks like this.

v=spf1 include:spf.smit.ee ip4:213.180.8.75 -all

By not having a DMARC record there is no guidelines from the domain owner on how to handle spoofed or otherwise suspicious emails from their domain. Thanks to the SPF record there is at least the possibility to check for the legitimacy of the origin of the email.

3.9.19 Conclusions

In 2020 I analysed 20 domains. Out of those 20 domains 19 had a DMARC record. 12 out of 19 domains had ‘reject’ as their main policy, 2 domains had ‘quarantine’ as their main policy and 5 domains had ‘none’ as their main policy. One domain had no DMARC record, but it had an SPF record.

Five domains had different policies for main domain and subdomain. Three of them had ‘reject’ as their policy for main domain and ‘none’ for subdomain. Two had ‘quarantine’ as their policy for main domain and ‘reject’ for subdomain. The first approach still allows for malicious emails to get through if a subdomain is used. The second approach only allows emails from the main domain and if there is a chance of misuse of the domain the email would be flagged or sent to spam. The first approach was used by Estonian Ministry of the Interior, Police and Ministry of Rural Affairs. The second approach was used by Estonian Defence Forces and NATO Cooperative Cyber Defence Centre of Excellence.

3.10 Comparison between 2019 and 2020 results

Comparison between 2019 and 2020 results show that the overall situation has improved as shown in Table 1. All the domains that did not have a DMARC record in 2019 had added a record by 2020. All the domains that had ‘none’ as their main policy in 2019 had changed it to something stricter by 2020 with two exceptions. The exceptions were Ministry of Economic Affairs and Communications and Ministry of Finance. Although the overall situation has improved there is still room for improvement. For example, those domains that had set ‘reject’ as their main policy but ‘none’ as their subdomain policy allow to use subdomains and the DMARC record instructs to do nothing with these kinds of emails.

Table 1. DMARC policy comparison.

Domain	**2019**		**2020**	
	p	**sp**	**p**	**sp**
eesti.ee	none	none	reject	reject
just.ee	none	none	reject	reject
kaitseministeerium.ee	-	-	reject	reject
mkm.ee	none	none	none	none
rahandusministeerium.ee	none	none	none	none
fin.ee	-	-	none	none
siseministeerium.ee	-	-	reject	none
politsei.ee	-	-	reject	none
mil.ee	none	none	quarantine	reject
emta.ee	none	none	reject	reject
rik.ee	none	none	reject	reject
ria.ee	none	none	reject	reject
ccdcoe.org	-	-	quarantine	reject
ccdcoe.ee	reject	reject	reject	reject
hm.ee			reject	reject
envir.ee			none	none
kul.ee			reject	reject
agri.ee			reject	none
sm.ee			none	none

Domain	**2019**		**2020**	
	p	**sp**	**p**	**sp**
vm.ee			**-**	**-**

4 Cambridge emails

To test how having or not having a DMARC record and policy being set up I looked thru and analysed emails from Cambridge University that had been confirmed to be sent with a malicious intent by the local cyber security team. There is also an incident report about every email that I analysed.

For information, CamCERT has now been reclassified from a CERT to a CSIRT from June 2019, and no longer provides 24-hour assistance.

There were incident reports about every email, and I will be mentioning the impact those emails had. The impact levels I mention are NIST impact levels.

4.1 Method

To analyse the emails, I manually looked thru 85 emails and categorized them by different qualities. I chose to use five main categories which were blackmail, credentials, personal data, malware, and trust establishment. I also collected the from and reply-to addresses and whether the domain the email was looking to have come from had a DMARC record and what the policy was.

4.1.1 Categories

Blackmail category is for emails that try to get people pay by threatening to publish certain material or information about the person.

Credentials category is for emails that try to get people to enter and submit their credentials for certain service or domain. That allows the attacker to get access to materials otherwise not available or take over an account to use it for some bigger goal. For example, gaining access to university accounts allows the attacker to download scientific papers that would otherwise need to be paid for and upload them to webpages that share them for free. An example is a page called pubmed007 [17].

Personal data category is for emails that try to get more data than just the credentials. It can mean address, phone number, full name and a picture of the person’s id or passport. This kind of information can be used to impersonate another person when filling out a form.

Malware category is for emails that are trying to infect machines with malware. This can be used to spread ransomware for example.

Trust establishment category is for emails that do not seem to be after anything certain at first glance. They explain who they are and what they are offering. These kinds of emails are waiting the target to start a conversation and by that the procedure seems more natural and normal. When the attacker finally decides to offer some goods for a good price then the target might feel safe enough to go thru with the deal.

4.1.2 From and reply-to addresses

From and reply-to addresses are a good indicator for a malicious intent. Attackers can use spoofing to pretend that the email is from a certain address when in fact it really is not. When it is important for the attacker to exchange emails with the target then the reply to the original email needs to be delivered to a different address and this is where the reply-to address comes into play. By viewing and comparing those addresses it can be asserted that there is a high probability that the email might have been sent with a malicious intent.

4.1.3 Presence of DMARC record

In order to test what role does DMARC play in malicious emails and what effect it might have I also checked the domains from each email. Since DMARC uses the ‘from’ address I took the domains from that field. To check the records, I used a domain checker on Dmarcian webpage [18]. I marked whether the domain had a DMARC record and what policy it had.

4.2 Findings

Out of the 85 emails six were blackmail, 31 were a phish for credentials, nine were a phish for personal data, 37 were malware and two were trust establishment.

4.2.1 Blackmail

All the blackmail emails had a similar style. Out of the six emails that were blackmail, five were trying to blackmail people based on having a video of them watching porn. All those emails claimed that the target had been infected with malware from a porn site they visited and had been observing the target’s activities. They then continued to claim that they had recorded both the target’s screen and webcam and were going to send it to all the target’s contacts that were also obtained from the device. The attacker continued by claiming that contacting the police has no point and when the asked amount has been transferred the video will be deleted. Every blackmail email had a bitcoin address to transfer the money.

One email out of the six was trying to blackmail the target into paying to save their life. In the email the attacker was saying that he had been hired to kill the target but would agree to cancel the hit and reveal information about who ordered the killing. The attacker claimed that he would do that for a much smaller amount compared to the original fee he was supposed to get.

What is interesting about these types of emails is that they make claims and threats without providing any real evidence for it. In the first cases there was some clever attempt by the attacker to use social media to try to claim the name of the target’s family member to be one of their passwords, but this turned out to be false. These emails probably work if the user has really done what is said in the email and they use fear and shame to make people pay.

Blackmail emails had the highest impact of all the categories. The impact was mostly emotional due to the nature of those attacks. (Annex 1)

4.2.2 Credentials

The credentials phishing was mainly based on different problems with the target’s mail account. The high number of credential phishing emails could be explained by the market for scientific papers that can be accessed with a university account [17]. The incident reports showed that this turned out to be the motivation behind most of the credential attacks. Out of the 31 emails 21 included a link in the email, as seen in Figure 3, which allows to create a legitimate looking fake page and direct the target to collect the credentials.

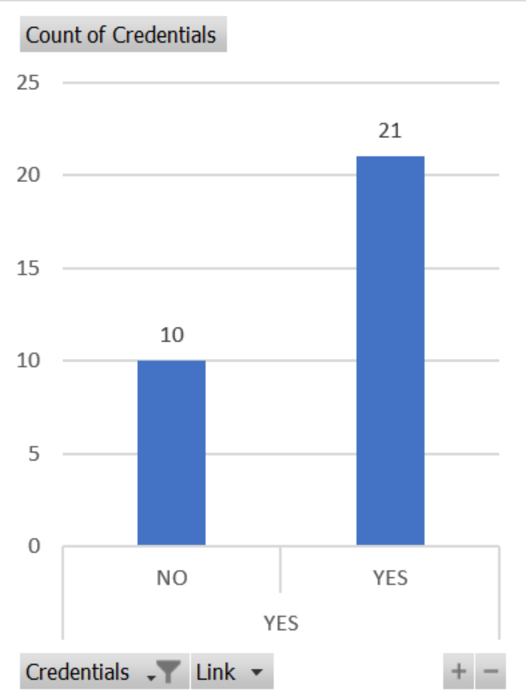


Figure 3. Count of credential emails and presence of link in the email.

There were two main types of credential phishing. The first type was where the attacker stated that the target's quota for sending or receiving messages was about to run out and the target needed to send or enter their credentials in order to renew the quota. The second type was where the attacker stated that they were updating the mail server and it was needed to upgrade the account by clicking the given link and entering credentials. (Annex 2)

4.2.3 Personal data

There were nine emails that were trying to get personal data from people. Two of the emails were claiming that the sender wanted to send some money or gold to the target. But in order to do so the sender needed some extra information about the target which included a picture of an identity document. The impact for two of the attacks was medium. (Annex 3)

4.2.4 Malware

Most of the emails were malware and it can be said that most of the malware emails were remarkably similar. Common claim made by the sender was that the target had received an invoice attached to the email. There were also claims about shared documents, tax return info, order sheets, miracle cures and package delivery. Every email had a link or an attached file to deliver the malware. Although malware was the most popular category among these emails the impact of those emails was mostly low. Only one email had a medium impact. (Annex 4)

4.2.5 Trust establishment

Trust establishment emails are similar to the personal data emails in the way that they need engaging from the target. These emails did not make any certain demands and they didn’t ask for anything. They were trying to give the impression of giving information about a good opportunity. Then if the target feels intrigued, it is much easier to continue with the communication and with building the trust needed to ask for money or other desired things. The impact for trust establishment emails was low. (Annex 5)

4.2.6 From and reply-to addresses

There were two emails that I was not able to find the ‘from’ address from. For others, the ‘from’ address was always present in the email. Even if someone had forwarded the email there was still the information about the original ‘from’ address at the beginning of the email.

I was not able to get ‘reply-to’ addresses for all emails. This was due to the way I received the emails. Some of them were the originals and some were email conversations of people forwarding them to the cyber security department of Cambridge University. Because of that the headers of the email or metadata was not present. This is because of a user problem when reporting emails for further investigation. This is because of the many ways to report header information in different email clients to CamCERT and this is very awkward, depending on the version of Outlook or alternative mail client they are using. [19] One way this could be improved is having a button on the email that says “forward for investigation” which would forward with full headers to their respective CERT and POSTMASTER.

For that reason, comparing and deciding whether the addresses differed did not have a concrete outcome. 13 emails had a different ‘reply-to’ address, 8 did not have and for 64 emails it could not be specified as seen if Figure 4. There could be both different and same ‘reply-to’ addresses among the 64 emails.

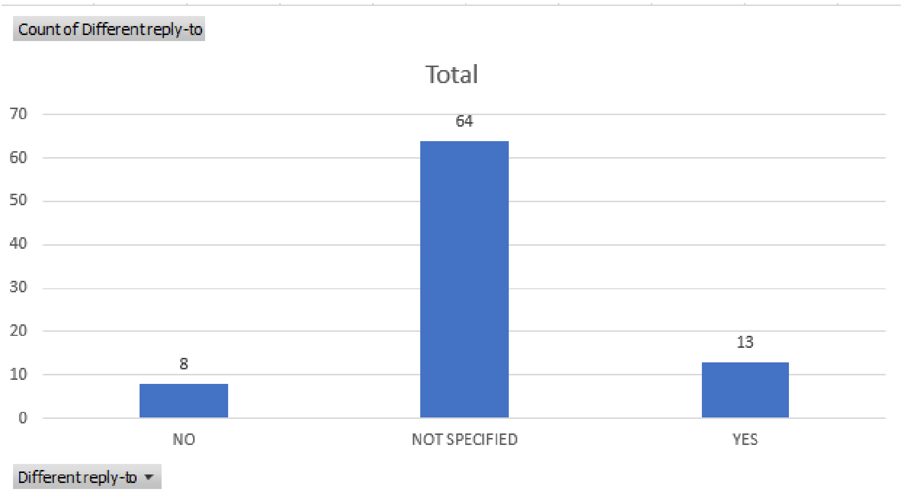


Figure 4. Count of different ‘reply-to’ addresses.

4.2.7 DMARC record

Since I could not get a ‘from’ address for two of the emails I excluded them from the DMARC analysis. Out of the 83 emails that had domains I could check 59 did not have a DMARC record. Out of the 24 emails that had a DMARC record for their domain 18 had set their policy to ‘none’ which allows emails to reach the recipient even if the checks fail. Only two had set their policy as ‘quarantine’ and four as rejected. The count of used DMARC policies can be seen in Figure 5.

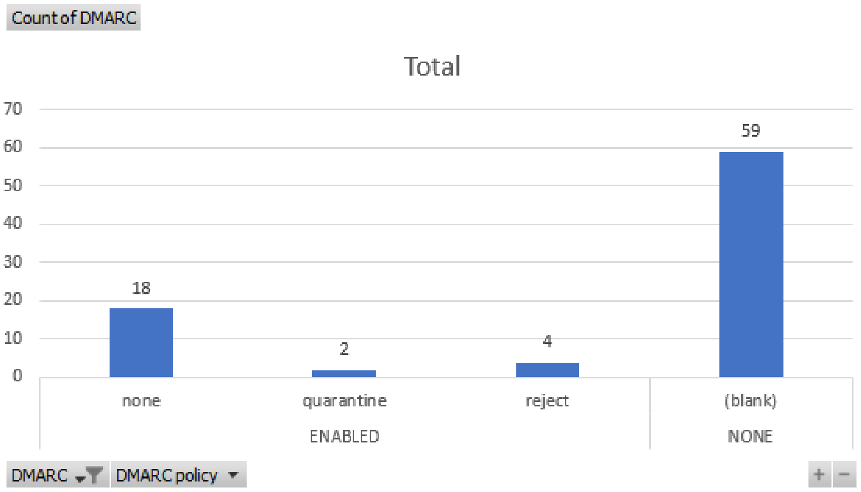


Figure 5. Count of DMARC policies.

When correlating the different ‘reply-to’ counts and DMARC policies it can be seen on Figure 6 that there seems to be more different ‘reply-to’ addresses that same among the emails where there was no DMARC record present. From that it can be deduced that domains that did not have a DMARC record were used more to spoof the ‘from’ address and deliver a malicious email.

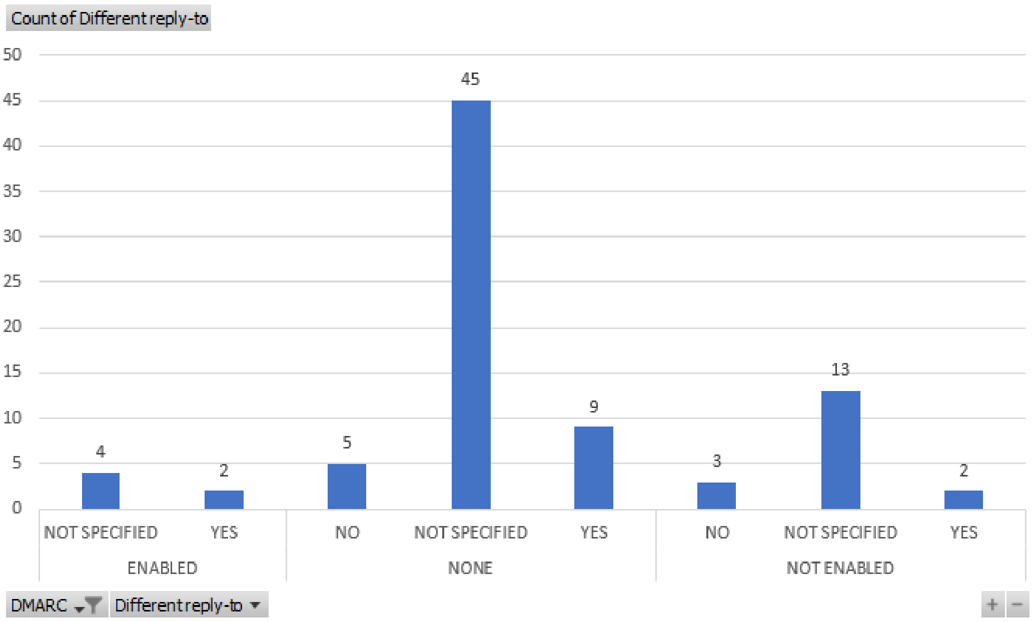


Figure 6. Correlation between DMARC policy and count of different reply-to.

I also correlated the DMARC records with whether the email account was probably spoofed or hacked and gave me the following information. It showed that for the domains that had a strict DMARC policy the account was either hacked or the attacker had spoofed the ‘from’ address to pretend to be someone else. The number of hacked or spoofed emails was the same.

When the policy was set to ‘none’, the number of spoofed emails grew compared to the hacked accounts. When there was no DMARC record for the domain then the number of spoofed emails grew even more while the number of hacked emails stayed the same. These comparisons can be seen on Figure 7.

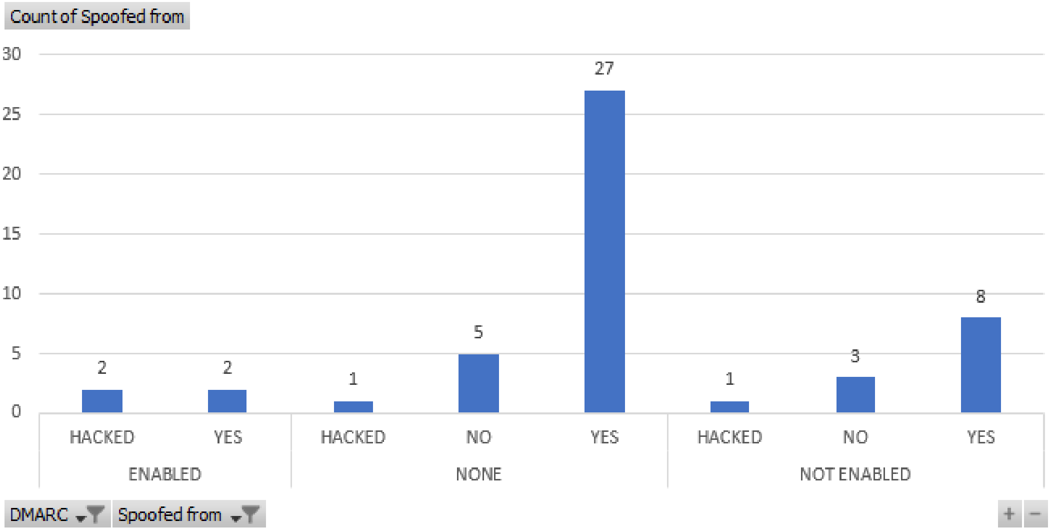


Figure 7. Correlation between DMARC policy and spoofing.

That also shows how not using DMARC drastically increases the chances that someone can use your domain by spoofing the ‘from’ address.

When I correlated DMARC usage with the impact from incident reports I found that emails that had high or medium impact did not have a DMARC record or DMARC policy was set to ‘none’ as can be seen in Figure 8.

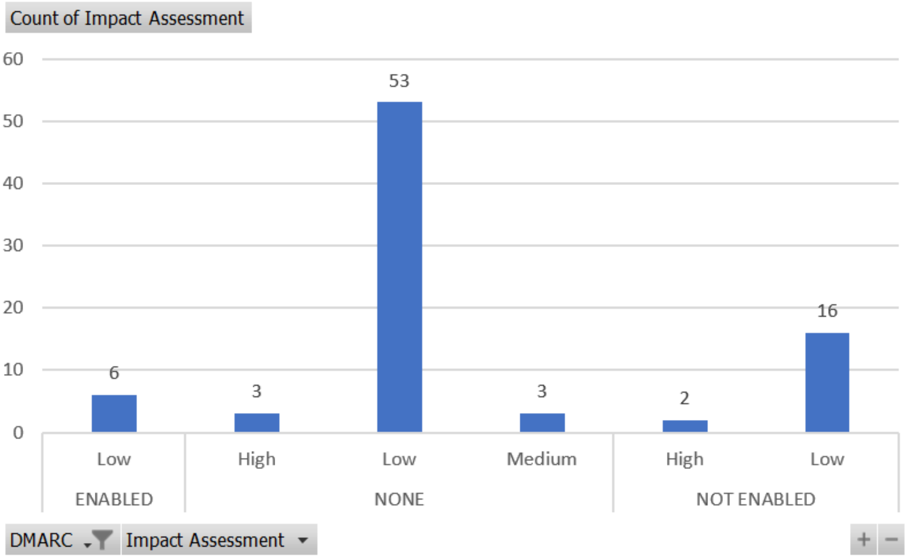


Figure 8. Correlation between DMARC policy and impact.

5 Summary

Estonia is known for its e-services which are implemented well and have caught the attention of other countries. By implementing services, other aspects might have been left unnoticed. Different government institutions that might have something to do with the services have domains that are not using DMARC or are using it in a way that is not fully embracing the possibilities of the method and opens the domains for a possible misuse.

By analysing 85 emails from Cambridge University that were confirmed as spam or phishing attacks it was possible to see what effect DMARC has. Universities have people from different ages and cultures and thus act as good models for a country. It turned out that the domains which did not have a DMARC record or had the policy set to 'none' were used more in successful phishing attacks by spoofing the sender address. That means that if your domain has a much bigger chance of being misused if you do not have a DMARC record for your domain.

It is also possible to have a DMARC record but to have little use of it due to misconfiguration or configuring it inefficiently. DMARC enables to specify email addresses to send feedback about domain misuse which allows the domain owner to see if and how much their domain is being misused. However, when the feedback email domain differs from the domain that DMARC is set for then special permission is needed to be set up. If that is skipped the feedback emails do not reach the appropriate instances. Furthermore, if the policy is set to 'none' to let emails thru and monitor the misuse cases using the feedback, the situation becomes almost as there is no DMARC present at all.

In case of Estonia, the results showed that there are problems with setting up DMARC correctly. That can be due to lack of knowledge or complexity of the systems. In my literature overview I mentioned a paper which found out that difficulty of setting up DMARC due to complexity of systems is a possible reason why DMARC is not adopted as widely as it could be [8]. In Estonia, there is the possibility for several cases of misuse. Ministry of Foreign Affairs has no DMARC record which makes it a good target for domain misuse. Ministry of Economic Affairs and Communications, Ministry of Finance, Ministry of the Environment and Ministry of Social Affairs have set DMARC with ‘none’ as their policy for their main domain. Out of those domains Ministry of Economic Affairs and Communications and Ministry of Social Affairs also have feedback addresses that are not verified. That allows to misuse those domains without the domain owner finding out about it. Ministry of the Interior, Police and Ministry of Rural Affairs have set their main policy as ‘reject’ but set their subdomain policy as ‘none’ which makes it seem like DMARC is set up and made to reject all emails that fail the checks but actually allows emails from subdomains to get thru. Also, both Ministry of the Interior and Police have feedback addresses that are not verified which allows to use those subdomains without the domain owner knowing about it. Although most of Estonian government institutions are using DMARC as recommended by the Information System Authority of Estonia [20], there are still institutions that need improving.

However, it also must be taken into account that the receiving end has to be checking for the DMARC record and doing all the needed checks in order for the method to have any effect.

References

[1] B. Seeman. [Online]. Available: https://www.advisorycloud.com/board-of-directors-articles/email-is-like-mailing-a-postcard. [Accessed 17 April 2019].

[2] "E-Estonia," [Online]. Available: https://e-estonia.com/. [Accessed 18 April 2019].

[3] E. Derouet, "Fighting phishing and securing data with email authentication," *Computer Fraud & Security,* vol. 2016, no. 10, pp. 5-8, 2016.

[4] Z. Durumeric, D. Adrian, J. Kasten, E. Bursztein, N. Lidzborski, K. Thomas, V. Eranti, M. D. Bailey and J. A. Halderman, "Neither Snow Nor Rain Nor MITM...: An Empirical Analysis of Email Delivery Security," in *IMC '15: Proceedings of the 2015 Internet Measurement Conference,* Tokyo, Japan, 2015.

[5] B. P. Dreller, G. J. Colburn and G. M. Bilbrey, "Real-time classification of email message traffic". United States Patent US9143476B2, 22 September 2015.

[6] M. Maass, P. Wichmann, H. Pridöhl and D. Herrmann, "PrivacyScore: Improving Privacy and Security via Crowd-Sourced Benchmarks of Websites," in *APF 2017: Privacy Technologies and Policy,* Vienna, 2017.

[7] A. Malatras, I. Coisel and I. Sanchez, "Technical recommendations for improving security of email communications," in *2016 39th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, Opatija, 2016.

[8] H. Hu, P. Peng and G. Wang, "Towards Understanding the Adoption of Anti-Spoofing Protocols in Email Systems," in *2018 IEEE Cybersecurity Development (SecDev),* Cambridge, MA, 2018.

[9] H. Hu, P. Peng and G. Wang, "Towards the Adoption of Anti-spoofing Protocols," 2017.

[10] H. Hu and G. Wang, "Revisiting Email Spoofing Attacks," 2018.

[11] M. Kucherawy and E. Zwicky, "Domain-based Message Authentication, Reporting, and Conformance (DMARC)," March 2015. [Online]. Available: https://www.rfc-editor.org/info/rfc7489. [Accessed 22 March 2019].

[12] P. Resnick, "Internet Message Format," 2008.

[13] S. Kitterman, "Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1," 2014.

[14] D. Crocker, T. Hansen and M. Kucherawy, "DomainKeys Identified Mail (DKIM) Signatures," 2011.

[15] "Rahandusministeeriumi kontaktid," [Online]. Available: https://www.rahandusministeerium.ee/et/kontakt. [Accessed 29 March 2019].

[16] "CCDCOE contacts," [Online]. Available: https://ccdcoe.org/contact/. [Accessed 9 April 2019].

[17] "pubmed007," [Online]. Available: http://pubmed007.com/. [Accessed 12 April 2019].

[18] "Dmarcian," [Online]. Available: https://dmarcian.com/domain-checker/. [Accessed 12 April 2019].

[19] U. o. Cambridge, "UIS How to forward headers," [Online]. Available: https://help.uis.cam.ac.uk/service/security/stay-safe-online/phishing/email-headers.

[20] I. S. Authority, "Trends and Challenges in Cyber Security," Information System Authority, 2018.

[21] "DMARC," [Online]. Available: https://dmarc.org/overview/. [Accessed 22 March 2019].

Appendix 1 – Example of a blackmail email

It appears that, (xxx23), is your password. You might not know me and you are probably wondering why you are getting this e mail, right?

in fact, I put in place a viruses on the adult vids (adult) website and guess what, you visited this web site to have fun (you know what What i'm saying is). During the time you were watching videos, your internet browser started out operating as a RDP (Remote Access) which provided me accessibility to your screen and web camera. from then on, my computer software obtained your complete contacts out of your Messenger, Outlook, FB, along with emails.

What did I really do?

I produced a double-screen video recording. First part shows the video you're watching (you have a good taste haha . . .), and Second part shows the recording of your web cam.

exactly what should you do?

Well, in my opinion, $1000 is a fair price for your little hidden secret. You will make the payment by Bitcoin (if you do not know this, search "how to buy bitcoin" search engines like google).

Bitcoin Address: 12nZnbCRwBoVaRVSLdpJGPLBLFBWuqyjoD

(It's case sensitive, so copy and paste it)

Important:

You've some days in order to make the payment. (I've a completely unique pixel within this e-mail, and at this moment I am aware you have read through this email message). If I don't get the BitCoins, I will certainly send out your videos to all of your contacts including family, co-workers, and so on. Having said that, if I get the payment, I'll destroy the video immidiately. If you need evidence, reply with "Yes!" and i'll undoubtedly mail out your video recording to your 6 contacts. It is a non-negotiable offer, that being said don't waste my personal time and yours by responding to this message.

Appendix 2 – Example of a credentials email

Hello,

This is to inform you that you have reached 80% of the mail box disk quota allocated. Please send the below information to us to re-activate and renew your quota

Full Email ID: ....

Password: ....

Failure to do so may result in limited access to your webmail account

Thanks

Local Host

Copyright 2018 - Webmail Communications - All Rights Reserved.

Appendix 3 – Example of a personal data email

Hello Sir,

My name is Mr.Solomon Mudani a banker in ECO bank here in mali, Please last eight months i deposited $2.8 million with 50 KG pure gold in bank of morocco, Now i want to quit from bank work and start a good investment but i needed good person who has current account for the bank to transfer the money also move the gold to the person. So are you willing or do you have anybody who will help out kindly let me know thanks and remain bless.

Hopping to hear from you soon.

Regards,

Mr.Solomon Mudani

Phone +223 63732017

Appendix 4 – Example of a malware email

Dear Sir,

We like to order from your company.

Please check the attached Order to see the products and quantities we need and quote your best selling price by issuing us Proforma Invoice accordingly.

We have also attached our company profile for your record.

I hope we can establish a long business relationship.

BISSELL International Trading Company

Address
BISSELL International Trading Company
Stadhouderskade 55
1072 AB Amsterdam Netherlands

Appendix 5 – Example of a trust establishment email

Hello,

Are you looking for a way to adjust your offer to the lifestyle of your customers and users?

Thanks to the skills of our programmers (591 specialists who graduated from the best Polish technical universities) and the use of high technology we can create top quality Java applications for your business. Thanks to them, you are going to meet the requirements of today's dynamic digital companies.

Our goal is simple: to build and implement an application as a way to improve your business and increase your income.

Let us know when we can make a quick phone call and define the goals of creation of a particular solution.

Piotr Korzeniowski